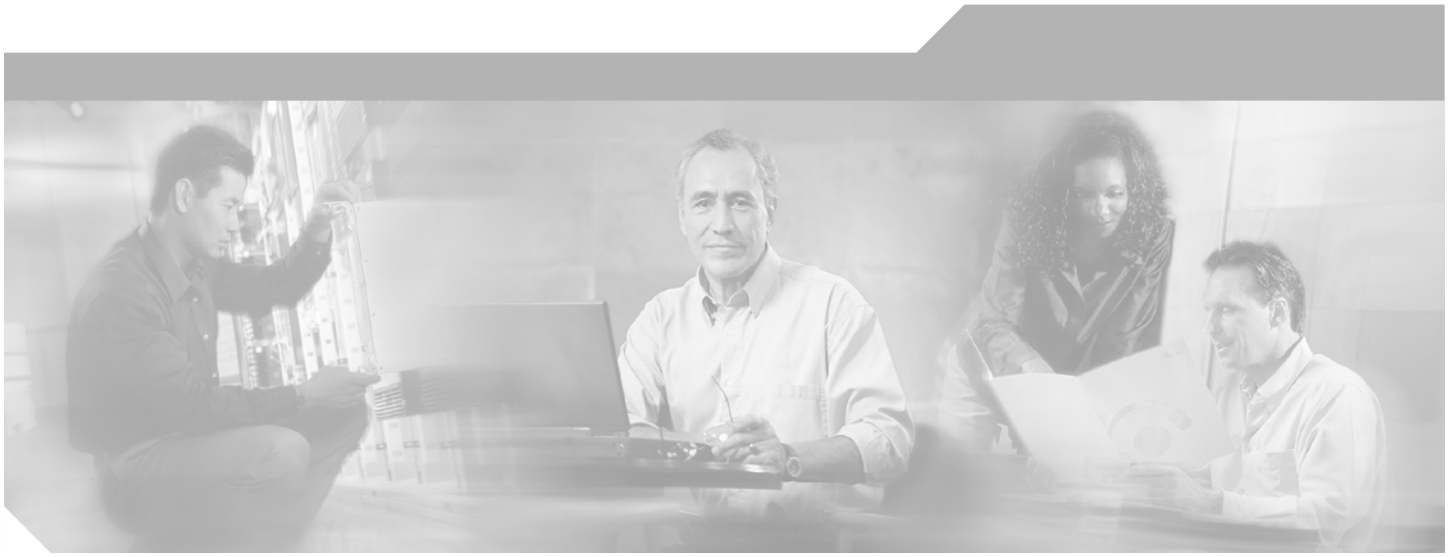


Cisco IOS Software Configuration Guide for Cisco Aironet Access Points

Cisco IOS Release 12.2(15)JA
April 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-5260-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)

Cisco IOS Software Configuration Guide for Cisco Aironet Access Points
Copyright © 2004 Cisco Systems, Inc.
All rights reserved.

CONTENTS

Preface xvii

- Audience xvii
- Purpose xvii
- Organization xvii
- Conventions xix
- Related Publications xxi
- Obtaining Documentation xxi
  - Cisco.com xxi
  - Documentation CD-ROM xxii
  - Ordering Documentation xxii
- Documentation Feedback xxii
- Obtaining Technical Assistance xxii
  - Cisco TAC Website xxiii
  - Opening a TAC Case xxiii
  - TAC Case Priority Definitions xxiii
- Obtaining Additional Publications and Information xxiv

CHAPTER 1 **Overview** 1-1

- Features 1-2
- Management Options 1-4
- Roaming Client Devices 1-4
- Network Configuration Examples 1-4
  - Root Unit on a Wired LAN 1-4
  - Repeater Unit that Extends Wireless Range 1-6
  - Central Unit in an All-Wireless Network 1-7

CHAPTER 2 **Configuring the Access Point for the First Time** 2-1

- Before You Start 2-2
  - Resetting the Access Point to Default Settings 2-2
- Obtaining and Assigning an IP Address 2-3
- Connecting to the 350 Series Access Point Locally 2-4
- Connecting to the 1100 Series Access Point Locally 2-5
- Connecting to the 1200 Series Access Point Locally 2-6

Assigning Basic Settings 2-6
Default Settings on the Express Setup Page 2-10
Configuring Basic Security Settings 2-11
Understanding Express Security Settings 2-12
Using VLANs 2-12
Express Security Types 2-12
Express Security Limitations 2-13
Using the Express Security Page 2-14
CLI Configuration Examples 2-14
Using the IP Setup Utility 2-19
Obtaining and Installing IPSU 2-20
Using IPSU to Find the Access Point's IP Address 2-20
Using IPSU to Set the Access Point's IP Address and SSID 2-21
Assigning an IP Address Using the CLI 2-23
Using a Telnet Session to Access the CLI 2-23

CHAPTER 3 **Using the Web-Browser Interface** 3-1
Using the Web-Browser Interface for the First Time 3-2
Using the Management Pages in the Web-Browser Interface 3-2
Using Action Buttons 3-4
Character Restrictions in Entry Fields 3-5
Using Online Help 3-5

CHAPTER 4 **Using the Command-Line Interface** 4-1
Cisco IOS Command Modes 4-2
Getting Help 4-3
Abbreviating Commands 4-3
Using no and default Forms of Commands 4-3
Understanding CLI Messages 4-4
Using Command History 4-4
Changing the Command History Buffer Size 4-4
Recalling Commands 4-5
Disabling the Command History Feature 4-5
Using Editing Features 4-5
Enabling and Disabling Editing Features 4-6
Editing Commands Through Keystrokes 4-6
Editing Command Lines that Wrap 4-7
Searching and Filtering Output of show and more Commands 4-8

Accessing the CLI 4-8
Opening the CLI with Telnet 4-8
Opening the CLI with Secure Shell 4-9

CHAPTER 5 **Administering the Access Point 5-1**
Preventing Unauthorized Access to Your Access Point 5-2
Protecting Access to Privileged EXEC Commands 5-2
Default Password and Privilege Level Configuration 5-2
Setting or Changing a Static Enable Password 5-3
Protecting Enable and Enable Secret Passwords with Encryption 5-4
Configuring Username and Password Pairs 5-5
Configuring Multiple Privilege Levels 5-6
Setting the Privilege Level for a Command 5-6
Logging Into and Exiting a Privilege Level 5-7
Controlling Access Point Access with RADIUS 5-7
Default RADIUS Configuration 5-8
Configuring RADIUS Login Authentication 5-8
Defining AAA Server Groups 5-9
Configuring RADIUS Authorization for User Privileged Access and Network Services 5-11
Displaying the RADIUS Configuration 5-12
Controlling Access Point Access with TACACS+ 5-12
Default TACACS+ Configuration 5-13
Configuring TACACS+ Login Authentication 5-13
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services 5-14
Displaying the TACACS+ Configuration 5-15
Configuring Ethernet Speed and Duplex Settings 5-15
Configuring the Access Point for Wireless Network Management 5-16
Configuring the Access Point for Local Authentication and Authorization 5-16
Configuring the Access Point to Provide DHCP Service 5-18
Setting up the DHCP Server 5-18
Monitoring and Maintaining the DHCP Server Access Point 5-19
Show Commands 5-19
Clear Commands 5-20
Debug Command 5-20
Configuring the Access Point for Secure Shell 5-20
Understanding SSH 5-20
Configuring SSH 5-21
Configuring Client ARP Caching 5-21

Understanding Client ARP Caching 5-21
Optional ARP Caching 5-22
Configuring ARP Caching 5-22
Managing the System Time and Date 5-22
Understanding the System Clock 5-23
Understanding Network Time Protocol 5-23
Configuring NTP 5-24
Default NTP Configuration 5-25
Configuring NTP Authentication 5-25
Configuring NTP Associations 5-27
Configuring NTP Broadcast Service 5-28
Configuring NTP Access Restrictions 5-29
Configuring the Source IP Address for NTP Packets 5-31
Displaying the NTP Configuration 5-32
Configuring Time and Date Manually 5-32
Setting the System Clock 5-33
Displaying the Time and Date Configuration 5-33
Configuring the Time Zone 5-34
Configuring Summer Time (Daylight Saving Time) 5-35
Configuring a System Name and Prompt 5-37
Default System Name and Prompt Configuration 5-37
Configuring a System Name 5-37
Understanding DNS 5-38
Default DNS Configuration 5-38
Setting Up DNS 5-39
Displaying the DNS Configuration 5-40
Creating a Banner 5-40
Default Banner Configuration 5-40
Configuring a Message-of-the-Day Login Banner 5-40
Configuring a Login Banner 5-42

CHAPTER 6 **Configuring Radio Settings** 6-1

Disabling and Enabling the Radio Interface 6-2
Configuring the Role in Radio Network 6-3
Configuring Radio Data Rates 6-4
Configuring Radio Transmit Power 6-6
Limiting the Power Level for Associated Client Devices 6-7
Configuring Radio Channel Settings 6-8
Enabling and Disabling World-Mode 6-10

Disabling and Enabling Short Radio Preambles 6-11
Configuring Transmit and Receive Antennas 6-11
Disabling and Enabling Aironet Extensions 6-12
Configuring the Ethernet Encapsulation Transformation Method 6-13
Enabling and Disabling Reliable Multicast to Workgroup Bridges 6-14
Enabling and Disabling Public Secure Packet Forwarding 6-15
Configuring Protected Ports 6-15
Configuring the Beacon Period and the DTIM 6-16
Configure RTS Threshold and Retries 6-16
Configuring the Maximum Data Retries 6-17
Configuring the Fragmentation Threshold 6-17
Enabling Short Slot Time for 802.11g Radios 6-18
Performing a Carrier Busy Test 6-18

CHAPTER 7 **Configuring Multiple SSIDs** 7-1
Understanding Multiple SSIDs 7-2
Configuring Multiple SSIDs 7-2
Default SSID Configuration 7-3
Creating an SSID 7-3
Using Spaces in SSIDs 7-4
Using a RADIUS Server to Restrict SSIDs 7-5

CHAPTER 8 **Configuring an Access Point as a Local Authenticator** 8-1
Understanding Local Authentication 8-2
Configuring a Local Authenticator 8-2
Guidelines for Local Authenticators 8-3
Configuration Overview 8-3
Configuring the Local Authenticator Access Point 8-3
Configuring Other Access Points to Use the Local Authenticator 8-6
Unblocking Locked Usernames 8-7
Viewing Local Authenticator Statistics 8-7
Using Debug Messages 8-7

CHAPTER 9 **Configuring Cipher Suites and WEP** 9-1
Understanding Cipher Suites and WEP 9-2
Configuring Cipher Suites and WEP 9-3
Creating WEP Keys 9-3

WEP Key Restrictions 9-4
Example WEP Key Setup 9-5
Enabling Cipher Suites and WEP 9-6
Matching Cipher Suites with WPA and CCKM 9-7
Enabling and Disabling Broadcast Key Rotation 9-7

CHAPTER 10 **Configuring Authentication Types** 10-1
Understanding Authentication Types 10-2
Open Authentication to the Access Point 10-2
Shared Key Authentication to the Access Point 10-3
EAP Authentication to the Network 10-3
MAC Address Authentication to the Network 10-5
Combining MAC-Based, EAP, and Open Authentication 10-6
Using CCKM for Authenticated Clients 10-6
Using WPA Key Management 10-7
Software and Firmware Requirements for WPA, CCKM, CKIP, and WPA-TKIP 10-8
Configuring Authentication Types 10-10
Default Authentication Settings 10-10
Assigning Authentication Types to an SSID 10-10
Configuring WPA Migration Mode 10-13
Configuring Additional WPA Settings 10-14
Configuring MAC Authentication Caching 10-15
Configuring Authentication Holdoffs, Timeouts, and Intervals 10-16
Matching Access Point and Client Device Authentication Types 10-17

CHAPTER 11 **Configuring WDS, Fast Secure Roaming, and Radio Management** 11-1
Understanding WDS 11-2
Role of the WDS Device 11-2
Role of Access Points Using the WDS Device 11-3
Understanding Fast Secure Roaming 11-3
Understanding Radio Management 11-4
Understanding Layer 3 Mobility 11-4
IP-Based Wireless Domain Services 11-5
Layer 3 Mobility Service Through Fast Secure Roaming Tunnels 11-5
Components Required for Layer 3 Mobility 11-5
Configuring WDS on the WLSM 11-6
Configuring WDS and Fast Secure Roaming 11-6
Guidelines for WDS 11-7
Requirements for WDS and Fast Secure Roaming 11-7

Configuration Overview 11-7
Configuring Access Points as Potential WDS Access Points 11-8
CLI Configuration Example 11-12
Configuring Access Points to use the WDS Device 11-13
CLI Configuration Example 11-14
Enabling Layer 3 Mobility on an SSID 11-15
CLI Configuration Example 11-15
Configuring the Authentication Server to Support Fast Secure Roaming 11-15
Viewing WDS Information 11-21
Using Debug Messages 11-22
Configuring Radio Management 11-23
CLI Configuration Example 11-24

CHAPTER 12 **Configuring RADIUS and TACACS+ Servers** 12-1
Configuring and Enabling RADIUS 12-2
Understanding RADIUS 12-2
RADIUS Operation 12-3
Configuring RADIUS 12-4
Default RADIUS Configuration 12-4
Identifying the RADIUS Server Host 12-4
Configuring RADIUS Login Authentication 12-7
Defining AAA Server Groups 12-9
Configuring RADIUS Authorization for User Privileged Access and Network Services 12-11
Starting RADIUS Accounting 12-12
Selecting the CSID Format 12-13
Configuring Settings for All RADIUS Servers 12-13
Configuring the Access Point to Use Vendor-Specific RADIUS Attributes 12-14
Configuring the Access Point for Vendor-Proprietary RADIUS Server Communication 12-15
Configuring WISPr RADIUS Attributes 12-16
Displaying the RADIUS Configuration 12-17
RADIUS Attributes Sent by the Access Point 12-18
Configuring and Enabling TACACS+ 12-21
Understanding TACACS+ 12-21
TACACS+ Operation 12-22
Configuring TACACS+ 12-22
Default TACACS+ Configuration 12-23
Identifying the TACACS+ Server Host and Setting the Authentication Key 12-23
Configuring TACACS+ Login Authentication 12-24
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services 12-25

Starting TACACS+ Accounting 12-26
Displaying the TACACS+ Configuration 12-27

CHAPTER 13 **Configuring VLANs** 13-1
Understanding VLANs 13-2
Related Documents 13-3
Incorporating Wireless Devices into VLANs 13-4
Configuring VLANs 13-4
Configuring a VLAN 13-4
Using a RADIUS Server to Assign Users to VLANs 13-6
Viewing VLANs Configured on the Access Point 13-6
VLAN Configuration Example 13-7

CHAPTER 14 **Configuring QoS** 14-1
Understanding QoS for Wireless LANs 14-2
QoS for Wireless LANs Versus QoS on Wired LANs 14-2
Impact of QoS on a Wireless LAN 14-3
Precedence of QoS Settings 14-3
Configuring QoS 14-4
Configuration Guidelines 14-4
Configuring QoS Using the Web-Browser Interface 14-4
Adjusting Radio Access Categories 14-8
Disabling IGMP Snooping Helper 14-10
Disabling AVVID Priority Mapping 14-10
QoS Configuration Examples 14-10
Giving Priority to Voice Traffic 14-10
Giving Priority to Video Traffic 14-12

CHAPTER 15 **Configuring Proxy Mobile IP** 15-1
Understanding Proxy Mobile IP 15-2
Overview 15-2
Components of a Proxy Mobile IP Network 15-2
How Proxy Mobile IP Works 15-3
Agent Discovery 15-3
Subnet Map Exchange 15-4
Registration 15-5
Tunneling 15-5
Proxy Mobile IP Security 15-6

Configuring Proxy Mobile IP 15-6
Configuration Guidelines 15-7
Configuring Proxy Mobile IP on Your Wired LAN 15-7
Configuring Proxy Mobile IP on Your Access Point 15-8

CHAPTER 16 **Configuring Filters** 16-1
Understanding Filters 16-2
Configuring Filters Using the CLI 16-2
Configuring Filters Using the Web-Browser Interface 16-2
Configuring and Enabling MAC Address Filters 16-3
Creating a MAC Address Filter 16-4
Using MAC Address ACLs to Block or Allow Client Association to the Access Point 16-5
CLI Configuration Example 16-8
Configuring and Enabling IP Filters 16-8
Creating an IP Filter 16-10
Configuring and Enabling Ethertype Filters 16-11
Creating an Ethertype Filter 16-12

CHAPTER 17 **Configuring CDP** 17-1
Understanding CDP 17-2
Configuring CDP 17-2
Default CDP Configuration 17-2
Configuring the CDP Characteristics 17-2
Disabling and Enabling CDP 17-3
Disabling and Enabling CDP on an Interface 17-4
Monitoring and Maintaining CDP 17-4

CHAPTER 18 **Configuring SNMP** 18-1
Understanding SNMP 18-2
SNMP Versions 18-2
SNMP Manager Functions 18-3
SNMP Agent Functions 18-3
SNMP Community Strings 18-3
Using SNMP to Access MIB Variables 18-4
Configuring SNMP 18-4
Default SNMP Configuration 18-5
Enabling the SNMP Agent 18-5
Configuring Community Strings 18-5

Configuring Trap Managers and Enabling Traps 18-7
Setting the Agent Contact and Location Information 18-9
Using the snmp-server view Command 18-9
SNMP Examples 18-9
Displaying SNMP Status 18-10

CHAPTER 19 **Configuring Repeater and Standby Access Points** 19-1
Understanding Repeater Access Points 19-2
Configuring a Repeater Access Point 19-3
Default Configuration 19-4
Guidelines for Repeaters 19-4
Setting Up a Repeater 19-4
Verifying Repeater Operation 19-5
Setting Up a Repeater As a LEAP Client 19-6
Setting Up a Repeater As a WPA Client 19-7
Understanding Hot Standby 19-8
Configuring a Hot Standby Access Point 19-8
Verifying Standby Operation 19-10

CHAPTER 20 **Managing Firmware and Configurations** 20-1
Working with the Flash File System 20-2
Displaying Available File Systems 20-2
Setting the Default File System 20-3
Displaying Information About Files on a File System 20-3
Changing Directories and Displaying the Working Directory 20-4
Creating and Removing Directories 20-4
Copying Files 20-5
Deleting Files 20-5
Creating, Displaying, and Extracting tar Files 20-6
Creating a tar File 20-6
Displaying the Contents of a tar File 20-6
Extracting a tar File 20-7
Displaying the Contents of a File 20-8
Working with Configuration Files 20-8
Guidelines for Creating and Using Configuration Files 20-9
Configuration File Types and Location 20-9
Creating a Configuration File by Using a Text Editor 20-10
Copying Configuration Files by Using TFTP 20-10
Preparing to Download or Upload a Configuration File by Using TFTP 20-10

Downloading the Configuration File by Using TFTP 20-11
Uploading the Configuration File by Using TFTP 20-11
Copying Configuration Files by Using FTP 20-12
Preparing to Download or Upload a Configuration File by Using FTP 20-13
Downloading a Configuration File by Using FTP 20-13
Uploading a Configuration File by Using FTP 20-14
Copying Configuration Files by Using RCP 20-15
Preparing to Download or Upload a Configuration File by Using RCP 20-16
Downloading a Configuration File by Using RCP 20-16
Uploading a Configuration File by Using RCP 20-17
Clearing Configuration Information 20-18
Deleting a Stored Configuration File 20-18
Working with Software Images 20-18
Image Location on the Access Point 20-19
tar File Format of Images on a Server or Cisco.com 20-19
Copying Image Files by Using TFTP 20-20
Preparing to Download or Upload an Image File by Using TFTP 20-20
Downloading an Image File by Using TFTP 20-21
Uploading an Image File by Using TFTP 20-22
Copying Image Files by Using FTP 20-23
Preparing to Download or Upload an Image File by Using FTP 20-23
Downloading an Image File by Using FTP 20-24
Uploading an Image File by Using FTP 20-26
Copying Image Files by Using RCP 20-27
Preparing to Download or Upload an Image File by Using RCP 20-27
Downloading an Image File by Using RCP 20-29
Uploading an Image File by Using RCP 20-31
Reloading the Image Using the Web Browser Interface 20-32
Browser HTTP Interface 20-32
Browser TFTP Interface 20-33

CHAPTER 21 **Configuring System Message Logging** 21-1
Understanding System Message Logging 21-2
Configuring System Message Logging 21-2
System Log Message Format 21-2
Default System Message Logging Configuration 21-3
Disabling and Enabling Message Logging 21-4
Setting the Message Display Destination Device 21-5
Enabling and Disabling Timestamps on Log Messages 21-6

Enabling and Disabling Sequence Numbers in Log Messages 21-6
Defining the Message Severity Level 21-7
Limiting Syslog Messages Sent to the History Table and to SNMP 21-8
Setting a Logging Rate Limit 21-9
Configuring UNIX Syslog Servers 21-10
Logging Messages to a UNIX Syslog Daemon 21-10
Configuring the UNIX System Logging Facility 21-10
Displaying the Logging Configuration 21-12

CHAPTER 22 **Troubleshooting** 22-1
Checking the Top Panel Indicators 22-2
Checking Basic Settings 22-5
SSID 22-5
WEP Keys 22-5
Security Settings 22-5
Resetting to the Default Configuration 22-5
Using the MODE Button 22-6
Using the Web Browser Interface 22-6
Using the CLI 22-7
Reloading the Access Point Image 22-8
Using the MODE button 22-8
Using the Web Browser Interface 22-9
Browser HTTP Interface 22-9
Browser TFTP Interface 22-10
Using the CLI 22-10
Obtaining the Access Point Image File 22-12
Obtaining TFTP Server Software 22-12

APPENDIX A **Channels and Antenna Settings** A-1
Channels A-2
IEEE 802.11b (2.4-GHz Band) A-2
IEEE 802.11g (2.4-GHz Band) A-3
IEEE 802.11a (5-GHz Band) A-4
Maximum Power Levels and Antenna Gains A-5
IEEE 802.11b (2.4-GHz Band) A-5
IEEE 802.11g (2.4-GHz Band) A-6
IEEE 802.11a (5-GHz Band) A-7

APPENDIX B **Protocol Filters** B-1

APPENDIX C **Supported MIBs** C-1

MIB List C-1

Using FTP to Access the MIB Files C-2

APPENDIX D **Error and Event Messages** D-1

Software Auto Upgrade Messages D-1

Association Management Messages D-2

Proxy Mobile IP Subsystem Messages D-2

Unzip Messages D-5

802.11 Subsystem Messages D-5

Inter-Access Point Protocol Messages D-9

Radio Diagnostic Messages D-10

GLOSSARY

INDEX

Preface

Audience

This guide is for the networking professional who installs and manages Cisco Aironet Access Points. To use this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of wireless local area networks.

Purpose

This guide provides the information you need to install and configure your access point. This guide provides procedures for using the Cisco IOS software commands that have been created or changed for use with the access point. It does not provide detailed information about these commands. For detailed information about these commands, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard Cisco IOS software commands, refer to the Cisco IOS software documentation set available from the Cisco.com home page at **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select **Release 12.2** from the Cisco IOS Software drop-down list.

This guide also includes an overview of the access point web-based interface (APWI), which contains all the funtionality of the command-line interface (CLI). This guide does not provide field-level descriptions of the APWI windows nor does it provide the procedures for configuring the access point from from the APWI. For all APWI window descriptions and procedures, refer to the access point online help, which is available from the Help buttons on the APWI pages.

Organization

This guide is organized into these chapters:

Chapter 1, "Overview," lists the software and hardware features of the access point and describes the access point's role in your network.

Chapter 2, "Configuring the Access Point for the First Time," describes how to configure basic settings on a new access point.

Chapter 3, "Using the Web-Browser Interface," describes how to use the web-browser interface to configure the access point.

Chapter 4, "Using the Command-Line Interface," describes how to use the command-line interface (CLI) to configure the access point.

Chapter 5, "Administering the Access Point," describes how to perform one-time operations to administer your access point, such as preventing unauthorized access to the access point, setting the system date and time, and setting the system name and prompt.

Chapter 6, "Configuring Radio Settings," describes how to configure settings for the access point radio such as the role in the radio network, data rates, transmit power, channel settings, and others.

Chapter 7, "Configuring Multiple SSIDs," describes how to configure and manage multiple service set identifiers (SSIDs) on your access point. You can configure up to 16 SSIDs on your access point and assign different configuration settings to each SSID.

Chapter 8, "Configuring an Access Point as a Local Authenticator," describes how to configure the access point to act as a local RADIUS server for your wireless LAN. If the WAN connection to your main RADIUS server fails, the access point acts as a backup server to authenticate wireless devices.

Chapter 9, "Configuring Cipher Suites and WEP," describes how to configure the cipher suites required to use authenticated key management, Wired Equivalent Privacy (WEP), and WEP features including MIC, CMIC, TKIP, CKIP, and broadcast key rotation.

Chapter 10, "Configuring Authentication Types," describes how to configure authentication types on the access point. Client devices use these authentication methods to join your network.

Chapter 11, "Configuring WDS, Fast Secure Roaming, and Radio Management," describes how to configure the access point to allow fast reassociation of roaming client devices. Using Cisco Centralized Key Management (CCKM) and an access point configured as a subnet context manager, client devices can roam from one access point to another without causing a delay in timing-sensitive applications, such as Voice over IP.

Chapter 12, "Configuring RADIUS and TACACS+ Servers," describes how to enable and configure the Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+), which provide detailed accounting information and flexible administrative control over authentication and authorization processes.

Chapter 13, "Configuring VLANs," describes how to configure your access point to interoperate with the VLANs set up on your wired LAN.

Chapter 14, "Configuring QoS," describes how to configure quality of service (QoS) on your access point. With this feature, you can provide preferential treatment to certain traffic at the expense of others.

Chapter 15, "Configuring Proxy Mobile IP," describes how to configure your access point's proxy mobile IP feature. When you enable proxy mobile IP on your access point and on your wired network, the access point helps client devices from other networks remain connected to their home networks.

Chapter 16, "Configuring Filters," describes how to configure and manage MAC address, IP, and Ethertype filters on the access point using the web-browser interface.

Chapter 17, "Configuring CDP," describes how to configure Cisco Discovery Protocol (CDP) on your access point. CDP is a device-discovery protocol that runs on all Cisco network equipment.

Chapter 18, "Configuring SNMP," describes how to configure the Simple Network Management Protocol (SNMP) on your access point.

Chapter 19, "Configuring Repeater and Standby Access Points," descibes how to configure your access point as a hot standby unit or as a repeater unit.

Chapter 20, "Managing Firmware and Configurations," describes how to manipulate the Flash file system, how to copy configuration files, and how to archive (upload and download) software images.

Chapter 21, "Configuring System Message Logging," describes how to configure system message logging on your access point.

Chapter 22, "Troubleshooting," provides troubleshooting procedures for basic problems with the access point.

Appendix A, "Channels and Antenna Settings," lists the access point radio channels and the maximum power levels supported by the world's regulatory domains.

Appendix B, "Protocol Filters," lists some of the protocols that you can filter on the access point.

Appendix C, "Supported MIBs," lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the access point supports for this software release.

Appendix D, "Error and Event Messages," lists the CLI error and event messages and provides an explanation and recommended action for each message.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and timesavers use these conventions and symbols:

Tip Means the following will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information.

Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means reader be careful. In this situation, you might do something that could result equipment damage or loss of data.

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")

Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)

Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)

Attention Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).

Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)

Avvertenza Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).

Advarsel Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)

Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

Related Publications

These documents provide complete information about the access point:

- *Quick Start Guide: Cisco Aironet 350 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1100 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1200 Series Access Points*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Installation Instructions for Cisco Aironet Power Injectors*
- *Cisco Aironet 802.11g Radio Upgrade Instructions*
- *Release Notes for 350, 1100, and 1200 Series Access Points for Cisco IOS Release 12.2(13)JA*

Click this link to browse to the Cisco Aironet documentation home page:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Click Subscriptions & Promotional Materials in the left navigation bar.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced user will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

Overview

Cisco Aironet Access Points (hereafter called *access points*) provide a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. With a management system based on Cisco IOS software, Cisco Aironet 350, 1100, and 1200 series access points are Wi-Fi certified, 802.11b-compliant, 802.11g-compliant, and 802.11a-compliant wireless LAN transceivers.

The 350 series access point, which can be upgraded to run Cisco IOS software, uses a single, 802.11b, 2.4-GHz mini-PCI radio. The 1100 series access point uses a single, 802.11b, 2.4-GHz mini-PCI radio that can be upgraded to an 802.11g, 2.4-GHz radio. The 1200 series access point can contain two radios: a 2.4-GHz radio in an internal mini-PCI slot and a 5-GHz radio module in an external, modified cardbus slot. The 1200 series access point supports one radio of each type, but it does not support two 2.4-GHz or two 5-GHz radios. You can configure the radios separately, using different settings on each radio.

Access points serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

You can configure and monitor the access point using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

This chapter provides information on the following topics:

- Features, page 1-2
- Management Options, page 1-4
- Roaming Client Devices, page 1-4
- Network Configuration Examples, page 1-4

Features

Access points running Cisco IOS software offer these software features:

- World mode—Use this feature to communicate the access point's regulatory setting information, including maximum transmit power and available channels, to world mode-enabled clients. Clients using world mode can be used in countries with different regulatory settings and automatically conform to local regulations. World mode is supported only on the 2.4-GHz radio.
- Repeater mode—Configure the access point as a wireless repeater to extend the coverage area of your wireless network.
- Standby mode—Configure the access point as a standby unit that monitors another access point and assumes its role in the network if the monitored access point fails.
- Multiple SSIDs—Create up to 16 SSIDs on your access point and assign any combination of these settings to each SSID:
  - Broadcast SSID mode for guests on your network
  - Client authentication methods
  - Maximum number of client associations
  - VLAN identifier
  - Proxy Mobile IP
  - RADIUS accounting list identifier
  - A separate SSID for infrastructure devices such as repeaters and workgroup bridges
- VLANs—Assign VLANs to the SSIDs on your access point (one VLAN per SSID) to differentiate policies and services among users.
- QoS—Use this feature to support quality of service for prioritizing traffic from the Ethernet to the access point. The access point also supports the voice-prioritization schemes used by 802.11b wireless phones such as Spectralink's Netlink™ and Symbol's Netvision™.
- Proxy Mobile IP—Use this feature to configure the access point to provide proxy Mobile IP service for clients that do not have mobile IP software installed.
- RADIUS Accounting—Enable accounting on the access point to send accounting data about wireless client devices to a RADIUS server on your network.
- TACACS+ adminstrator authentication—Enable TACACS+ for server-based, detailed accounting information and flexible administrative control over authentication and authorization processes. It provides secure, centralized validation of administrators attempting to gain access to your access point.
- Enhanced security—Enable three advanced security features to protect against sophisticated attacks on your wireless network's WEP keys: Message Integrity Check (MIC), WEP key hashing, and broadcast WEP key rotation.
- Enhanced authentication services—Set up repeater access points to authenticate to your network like other wireless client devices. After you provide a network username and password for the repeater, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys.

- Wi-Fi Protected Access (WPA)—Wi-Fi Protected Access is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.
- Fast secured roaming using Cisco Centralized Key Management (CCKM)—Using CCKM, authenticated client devices can roam securely from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.
- Access point as backup or stand-alone authentication server—You can configure an access point to act as a local authentication server to provide authentication service for small wireless LANs without a RADIUS server or to provide backup authentication service in case of a WAN link or a server failure. The access point can authenticate up to 50 LEAP-enabled wireless client devices and allow them to join your network. Access points running Cisco IOS Release 12.2(15)JA also can provide backup MAC-address authentication service for up to 50 addresses.
- Client ARP caching—To reduce traffic on the wireless LAN, you can configure access points running Cisco IOS Release 12.2(13)JA or later to reply to ARP queries on behalf of associated client devices. In previous releases, the access point forwards ARP queries to all associated client devices, and the specified client responds with its MAC address. When the access point maintains an ARP cache, however, it responds to ARP queries on behalf of the client device and does not forward the queries through its radio port.
- CCKM voice clients and WPA clients on the same VLAN—Access points running Cisco IOS Release 12.2(13)JA or later allow both 802.11b CCKM voice clients and 802.11b WPA clients on the same VLAN.
- WISPr RADIUS attributes—The Wi-Fi Alliance's WISPr *Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document lists RADIUS attributes that access points must send with RADIUS accounting and authentication requests. You can configure access points running Cisco IOS Release 12.2(13)JA or later to include these attributes in all RADIUS accounting and authentication requests.
- Support for 802.11g radios—Cisco IOS Releases 12.2(13)JA or later support the 802.11g, 2.4-GHz mini-PCI radio. You can upgrade the 802.11b, 2.4-GHz radio in 1100 and 1200 series access points with an 802.11g, 2.4-GHz radio.
- Radio management features on 802.11a, 802.11b, and 802.11g radios—Access points running Cisco IOS Release 12.2(15)JA can participate in radio management using 802.11a, b, and g radios. Access points configured for WDS interact with the WDS device on your wireless LAN. The WDS device forwards radio data to and from the WLSE device or wireless network manager on your network. Radio management includes these features, which are configured on your WLSE device:
  - Rogue access point detection, including the rogue device's IP and MAC addresses, SSID, and, if it is connected to a Cisco device, the switch port to which the rogue is connected
  - Self-healing wireless LAN; if an access point fails, nearby access points increase their transmit power to cover the gap in your wireless LAN
  - Client tracking to identify the access point to which each client device is associated
- Scanning-only mode—Access points running Cisco IOS Release 12.2(15)JA can act as scanners to detect rogue access points and monitor radio traffic on your wireless LAN. Access points configured as scanners participate in radio management but do not accept client associations.

Management Options

You can use the access point management system through the following interfaces:

- The Cisco IOS command-line interface (CLI), which you use through a Telnet session. Most of the examples in this manual are taken from the CLI. Chapter 4, "Using the Command-Line Interface," provides a detailed description of the CLI.
- A web-browser interface, which you use through a web browser. Chapter 3, "Using the Web-Browser Interface," provides a detailed description of the web-browser interface.
- Simple Network Management Protocol (SNMP). Chapter 18, "Configuring SNMP," explains how to configure your access point for SNMP management.

Roaming Client Devices

If you have more than one access point in your wireless LAN, wireless client devices can roam seamlessly from one access point to another. The roaming functionality is based on signal quality, not proximity. When a client's signal quality drops, it roams to another access point.

Wireless LAN users are sometimes concerned when a client device stays associated to a distant access point instead of roaming to a closer access point. However, if a client's signal to a distant access point remains strong and the signal quality is high, the client will not roam to a closer access point. Checking constantly for closer access points would be inefficient, and the extra radio traffic would slow throughput on the wireless LAN.

Using CCKM and a device providing Wireless Domain Services (WDS), client devices can roam from one access point to another so quickly that there is no perceptible delay in voice or other time-sensitive applications.

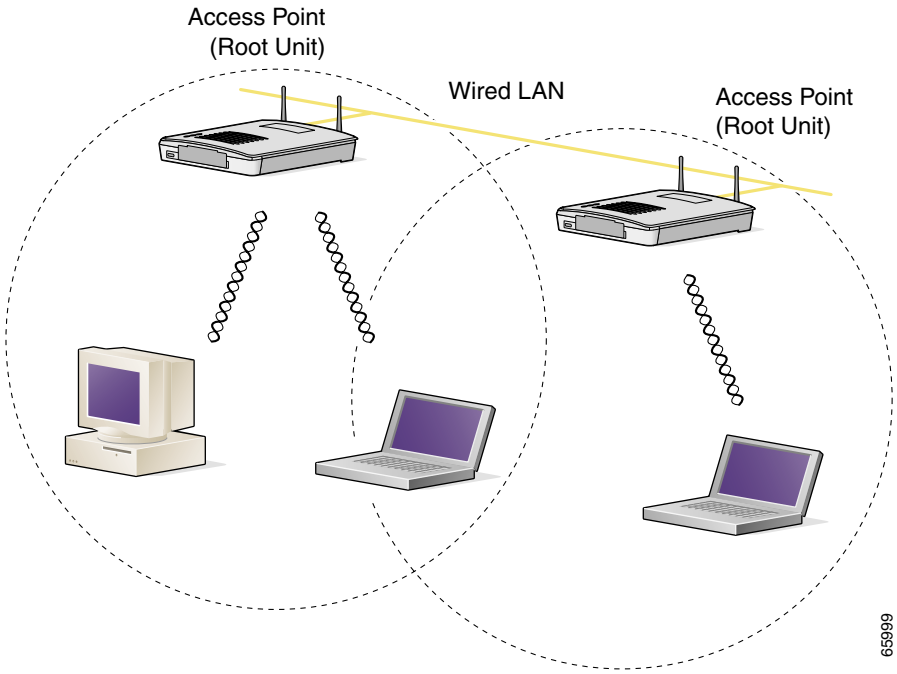
Network Configuration Examples

This section describes the access point's role in common wireless network configurations. The access point's default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. The repeater role requires a specific configuration.

Root Unit on a Wired LAN

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1-1 shows access points acting as root units on a wired LAN.

Figure 1-1 Access Points as Root Units on a Wired LAN

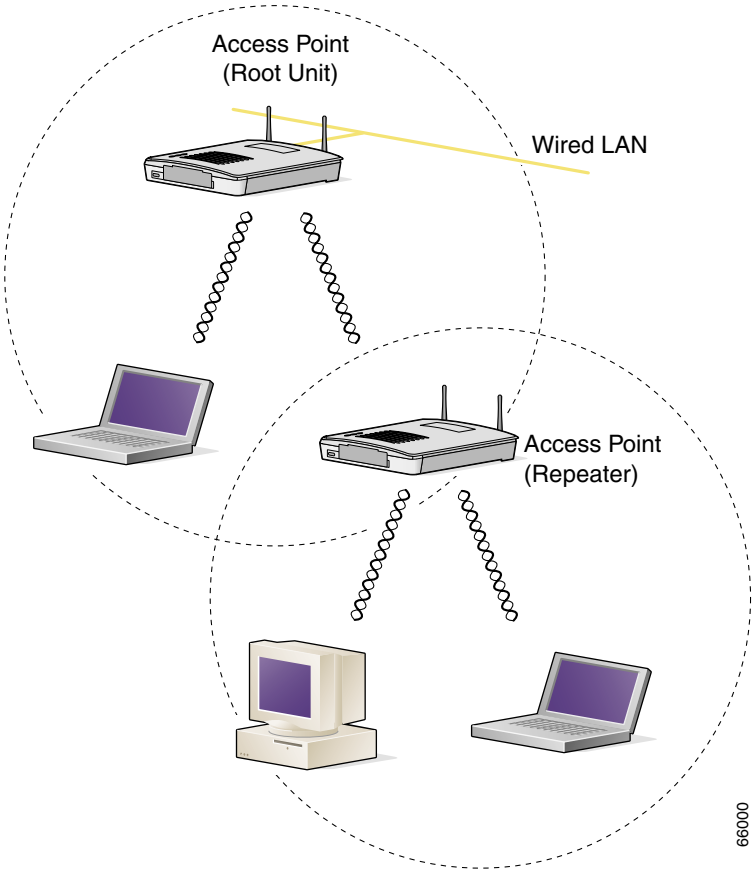


Repeater Unit that Extends Wireless Range

An access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. Figure 1-2 shows an access point acting as a repeater. Consult the "Configuring a Repeater Access Point" section on page 19-3 for instructions on setting up an access point as a repeater.

Note Non-Cisco client devices might have difficulty communicating with repeater access points.

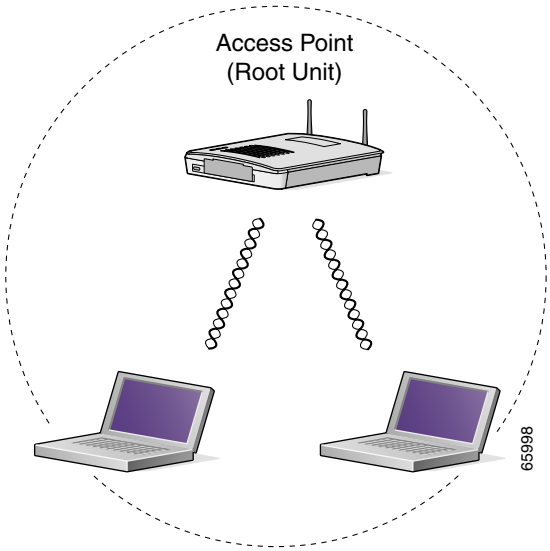
Figure 1-2 Access Point as Repeater



Central Unit in an All-Wireless Network

In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure 1-3 shows an access point in an all-wireless network.

Figure 1-3 Access Point as Central Unit in All-Wireless Network



CHAPTER 2

Configuring the Access Point for the First Time

This chapter describes how to configure basic settings on your access point for the first time. The contents of this chapter are similar to the instructions in the quick start guide that shipped with your access point. You can configure all the settings described in this chapter using the CLI, but it might be simplest to browse to the access point's web-browser interface to complete the initial configuration and then use the CLI to enter additional settings for a more detailed configuration.

This chapter contains these sections:

- Before You Start, page 2-2
- Obtaining and Assigning an IP Address, page 2-3
- Connecting to the 350 Series Access Point Locally, page 2-4
- Connecting to the 1100 Series Access Point Locally, page 2-5
- Connecting to the 1200 Series Access Point Locally, page 2-6
- Assigning Basic Settings, page 2-6
- Configuring Basic Security Settings, page 2-11
- Using the IP Setup Utility, page 2-19
- Assigning an IP Address Using the CLI, page 2-23
- Using a Telnet Session to Access the CLI, page 2-23

Before You Start

Before you install the access point, make sure you are using a computer connected to the same network as the access point, and obtain the following information from your network administrator:

- A system name for the access point
- The case-sensitive wireless service set identifier (SSID) for your radio network
- If not connected to a DHCP server, a unique IP address for your access point (such as 172.17.255.115)
- If the access point is not on the same subnet as your PC, a default gateway address and subnet mask
- A Simple Network Management Protocol (SNMP) community name and the SNMP file attribute (if SNMP is in use)
- If you use IPSU to find or assign the access point IP address, the MAC address from the label on the bottom of the access point (such as 00164625854c)

Resetting the Access Point to Default Settings

If you need to start over during the initial setup process, follow these steps to reset the access point to factory default settings using the access point MODE button:

Step 1 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 2 Press and hold the MODE button while you reconnect power to the access point.

Step 3 Hold the MODE button until the Status LED turns amber (approximately 1 to 2 seconds), and release the button. All access point settings return to factory defaults.

Note You cannot use the MODE button to reset 350 series access points to default settings. Use the web-browser interface to reset a 350 series access point to default settings, or follow the instructions in the "Using the CLI" section on page 22-7.

Follow these steps to return to default settings using the web-browser interface:

Step 1 Open your Internet browser. The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password window appears.

Step 3 Enter your username in the User Name field. The default username is **Cisco**.

Step 4 Enter the access point password in the Password field and press **Enter**. The default password is **Cisco**. The Summary Status page appears.

Step 5 Click **System Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

Step 7 Click the **Reset to Defaults** button.

Note If the access point is configured with a static IP address, the IP address does not change. If the access point is not configured with a static IP address, the access point requests a DHCP address. If it does not receive an address from a DHCP server, its IP address is 10.0.0.1.

Obtaining and Assigning an IP Address

To browse to the access point's Express Setup page, you must either obtain or assign the access point's IP address using one of the following methods:

- Use default address 10.0.0.1 when you connect to the access point locally. For detailed instructions, see the "Connecting to the 1100 Series Access Point Locally" section on page 2-5.
- If you have a 350 or a 1200 series access point, connect to the access point console port and assign a static IP address. Follow the steps in the"Connecting to the 350 Series Access Point Locally" section on page 2-4 or in the "Connecting to the 1200 Series Access Point Locally" section on page 2-6 to connect to the console port.
- Use a DHCP server (if available) to automatically assign an IP address. You can find out the DHCP-assigned IP address using one of the following methods:
  - If you have a 350 or a 1200 series access point, connect to the access point console port and use the **show ip interface brief** command to display the IP address. Follow the steps in the"Connecting to the 350 Series Access Point Locally" section on page 2-4 or in the "Connecting to the 1200 Series Access Point Locally" section on page 2-6 to connect to the console port.
  - Provide your organization's network administrator with your access point's Media Access Control (MAC) address. Your network administrator will query the DHCP server using the MAC address to identify the IP address. The access point's MAC address is on label attached to the bottom of the access point.
  - Use the Cisco IP Setup Utility (IPSU) to identify the assigned address. You can also use IPSU to assign an IP address to the access point if it did not receive an IP address from the DHCP server. IPSU runs on most Microsoft Windows operating systems: Windows 9x, 2000, Me, NT, and XP.

    You can download IPSU from the Software Center on Cisco.com. Click this link to browse to the Software Center:

    http://www.cisco.com/public/sw-center/sw-wireless.shtml

Connecting to the 350 Series Access Point Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its RS-232 console port using a nine-pin, male-to-female, straight-through serial cable. Follow these steps to open the CLI by connecting to the access point console port:

Step 1 Connect a nine-pin, male-to-female, straight-through DB-9 serial cable to the RS-232 serial port on the access point and to the COM port on a computer. Figure 2-3 shows the serial port connection.

Figure 2-1 Connecting the Serial Cable (Access Point with Plastic Case)

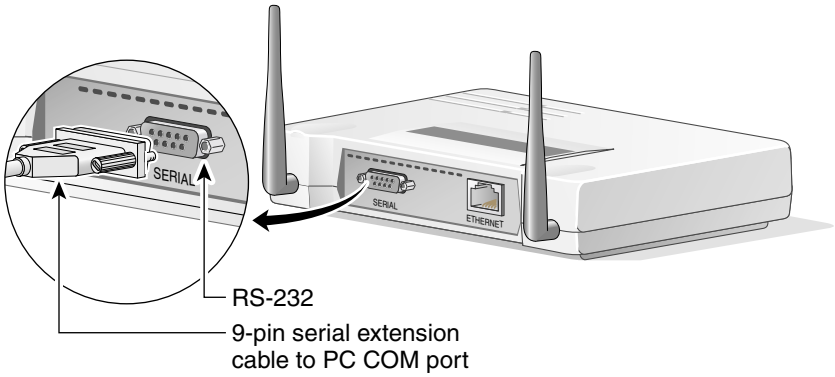
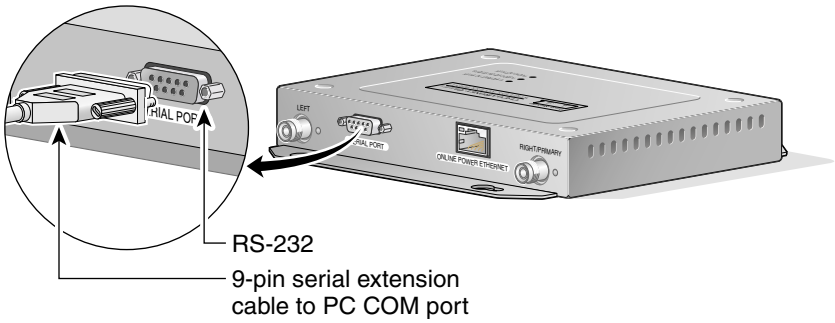


Figure 2-2 Connecting the Serial Cable (Access Point with Metal Case)



Step 2 Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and Xon/Xoff flow control.

Connecting to the 1100 Series Access Point Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its Ethernet port using a Category 5 Ethernet cable. You can use a local connection to the Ethernet port much as you would use a serial port connection.

Note You do not need a special crossover cable to connect your PC to the access point; you can use either a straight-through cable or a crossover cable.

If the access point is configured with default values and not connected to a DHCP server or cannot obtain an IP address, it defaults to IP address 10.0.0.1 and becomes a mini-DHCP server. In that capacity, the access point provides up to twenty IP addresses between 10.0.0.11 and 10.0.0.30 to the following devices:

- An Ethernet-capable PC connected to its Ethernet port
- Wireless client devices configured to use either no SSID or *tsunami* as the SSID, and with all security settings disabled

The mini-DHCP server feature is disabled automatically when you assign a static IP address to the access point.

Caution When an access point with default settings is connected on a wired LAN and does not receive an IP address from a DHCP server, the access point provides an IP address to any DHCP requests it receives.

Follow these steps to connect to the access point locally:

Step 1 Make sure that the PC you intend to use is configured to obtain an IP address automatically, or manually assign it an IP address from 10.0.0.2 to 10.0.0.10. Connect your PC to the access point using a Category 5 Ethernet cable. You can use either a crossover cable or a straight-through cable.

Step 2 Power up the access point.

Step 3 Follow the steps in the "Assigning Basic Settings" section on page 2-6. If you make a mistake and need to start over, follow the steps in the "Resetting the Access Point to Default Settings" section on page 2-2.

Step 4 After configuring the access point, remove the Ethernet cable from your PC and connect the access point to your wired LAN.

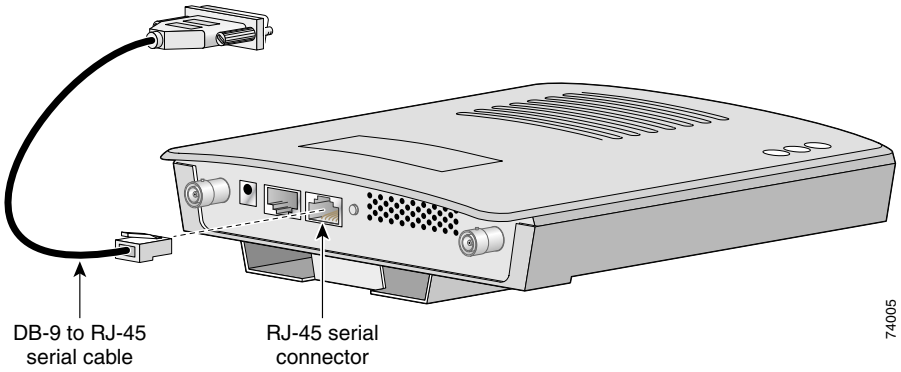
Note When you connect your PC to the access point or reconnect your PC to the wired LAN, you might need to release and renew the IP address on the PC. On most PCs, you can perform a release and renew by rebooting your PC or by entering **ipconfig /release** and **ipconfig /renew** commands in a command prompt window. Consult your PC operating instructions for detailed instructions.

Connecting to the 1200 Series Access Point Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable. Follow these steps to open the CLI by connecting to the access point console port:

Step 1 Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer. Figure 2-3 shows the serial port connection.

Figure 2-3 Connecting the Serial Cable



Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to http://www.cisco.com/go/marketplace to order a serial cable.

Step 2 Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Assigning Basic Settings

After you determine or assign the access point's IP address, you can browse to the access point's Express Setup page and perform an initial configuration:

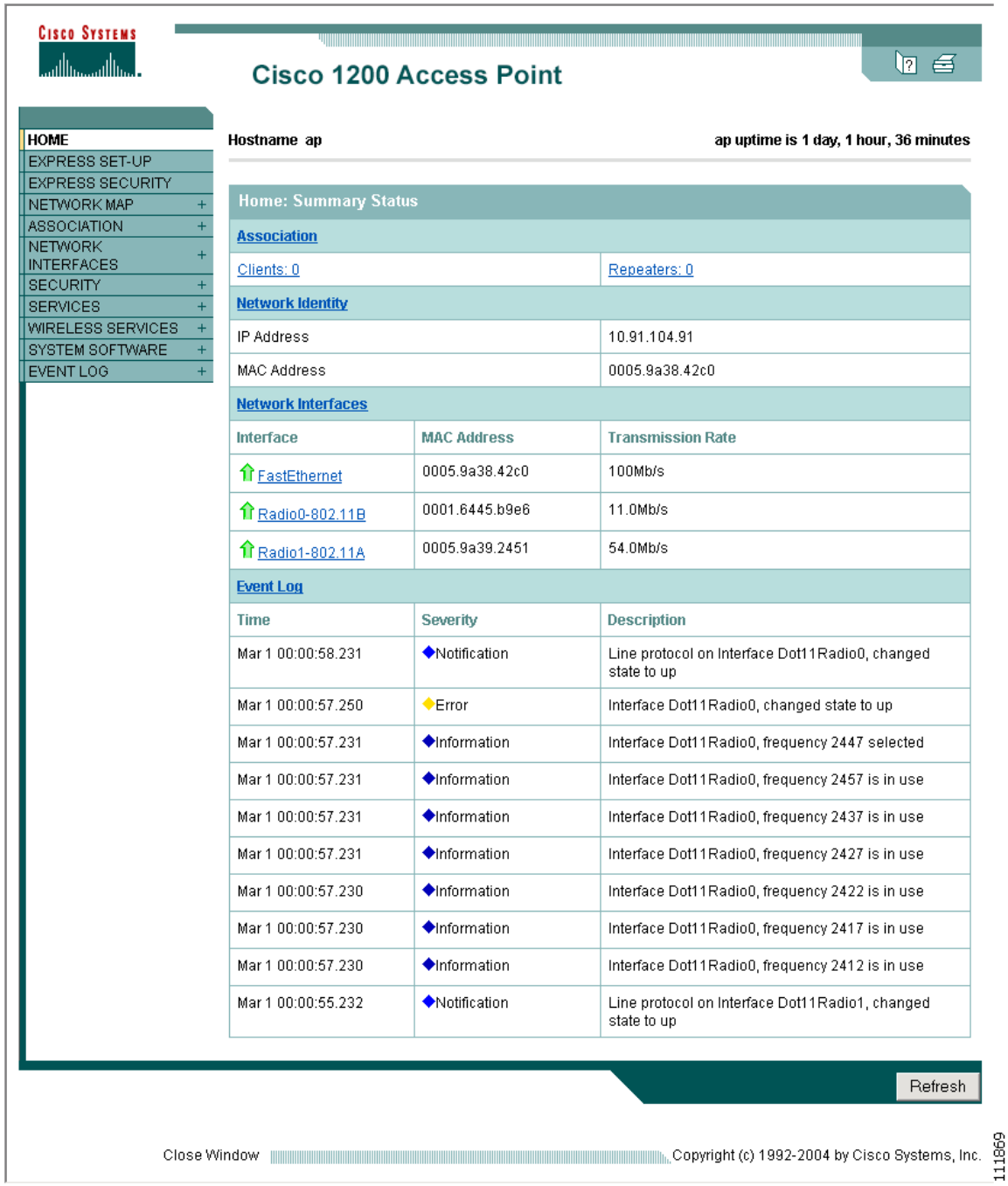
Step 1 Open your Internet browser. The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Press **Tab** to bypass the Username field and advance to the Password field.

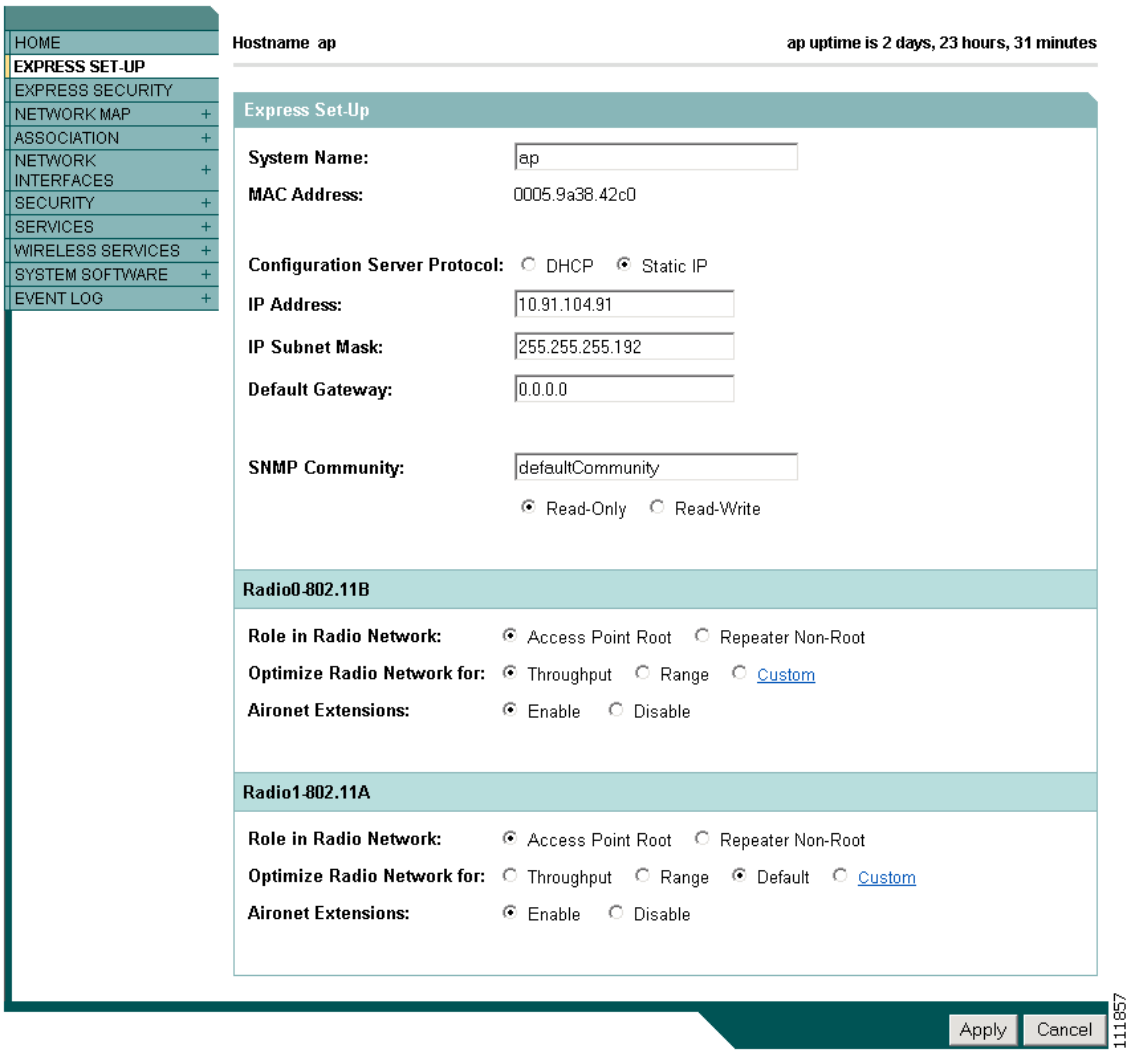
Step 4 Enter the case-sensitive password *Cisco* and press **Enter**. The Summary Status page appears. Figure 2-4 shows the Summary Status page.

Figure 2-4 Summary Status Page


Cisco Systems
Cisco 1200 Access Point
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +
Hostname ap
ap uptime is 1 day, 1 hour, 36 minutes
Home: Summary Status
Association
Clients: 0
Repeaters: 0
Network Identity
IP Address 10.91.104.91
MAC Address 0005.9a38.42c0
Network Interfaces
Interface MAC Address Transmission Rate
FastEthernet 0005.9a38.42c0 100Mb/s
Radio0-802.11B 0001.6445.b9e6 11.0Mb/s
Radio1-802.11A 0005.9a39.2451 54.0Mb/s
Event Log
Time Severity Description
Mar 1 00:00:58.231 Notification Line protocol on Interface Dot11Radio0, changed state to up
Mar 1 00:00:57.250 Error Interface Dot11Radio0, changed state to up
Mar 1 00:00:57.231 Information Interface Dot11Radio0, frequency 2447 selected
Mar 1 00:00:57.231 Information Interface Dot11Radio0, frequency 2457 is in use
Mar 1 00:00:57.231 Information Interface Dot11Radio0, frequency 2437 is in use
Mar 1 00:00:57.231 Information Interface Dot11Radio0, frequency 2427 is in use
Mar 1 00:00:57.230 Information Interface Dot11Radio0, frequency 2422 is in use
Mar 1 00:00:57.230 Information Interface Dot11Radio0, frequency 2417 is in use
Mar 1 00:00:57.230 Information Interface Dot11Radio0, frequency 2412 is in use
Mar 1 00:00:55.232 Notification Line protocol on Interface Dot11Radio1, changed state to up
Refresh
Close Window
Copyright (c) 1992-2004 by Cisco Systems, Inc.
111869

Step 5 Click **Express Setup**. The Express Setup screen appears. Figure 2-5 shows the Express Setup page.

Figure 2-5 Express Setup Page



Step 6 Enter the configuration settings you obtained from your system administrator. The configurable settings include:

- **System Name**— The system name, while not an essential setting, helps identify the access point on your network. The system name appears in the titles of the management system pages.

Note You can enter up to 32 characters for the system name. However, when the access point identifies itself to client devices, it uses only the first 15 characters in the system name. If it is important for client users to distinguish between access points, make sure a unique portion of the system name appears in the first 15 characters.

Note When you change the system name, the access point resets the radios, causing associated client devices to disassociate and quickly reassociate.

- **Configuration Server Protocol**—Click on the button that matches the network's method of IP address assignment.
  - **DHCP**—IP addresses are automatically assigned by your network's DHCP server.
  - **Static IP**—The access point uses a static IP address that you enter in the IP address field.
- **IP Address**—Use this setting to assign or change the access point's IP address. If DHCP is enabled for your network, leave this field blank.

Note If the access point's IP address changes while you are configuring the access point using the web-browser interface or a Telnet session over the wired LAN, you lose your connection to the access point. If you lose your connection, reconnect to the access point using its new IP address. Follow the steps in the "Resetting the Access Point to Default Settings" section on page 2-2 if you need to start over.

- **IP Subnet Mask**—Enter the IP subnet mask provided by your network administrator so the IP address can be recognized on the LAN. If DHCP is enabled, leave this field blank.
- **Default Gateway**—Enter the default gateway IP address provided by your network administrator. If DHCP is enabled, leave this field blank.
- **Role in Radio Network**—Click on the button that describes the role of the access point on your network. Select **Access Point (Root)** if your access point is connected to the wired LAN. Select **Repeater (Non-Root)** if it is not connected to the wired LAN.
- **Optimize Radio Network for**—Use this setting to select either preconfigured settings for the access point radio or customized settings for the access point radio.
  - **Throughput**—Maximizes the data volume handled by the access point but might reduce its range.
  - **Range**—Maximizes the access point's range but might reduce throughput.
  - **Custom**—The access point uses settings you enter on the Network Interfaces: Radio-802.11b Settings page. Clicking **Custom** takes you to the Network Interfaces: Radio-802.11b Settings page.
- **Aironet Extensions**—Enable this setting if there are only Cisco Aironet devices on your wireless LAN.
- **SNMP Community**—If your network is using SNMP, enter the SNMP Community name provided by your network administrator and select the attributes of the SNMP data (also provided by your network administrator).

Step 7 Click **Apply** to save your settings. If you changed the IP address, you lose your connection to the access point. Browse to the new IP address to reconnect to the access point.

Your access point is now running but probably requires additional configuring to conform to your network's operational and security requirements. Consult the chapters in this manual for the information you need to complete the configuration.

Note You can restore 1100 and 1200 series access points to factory defaults by unplugging the power jack and plugging it back in while holding down the Mode button for a few seconds, or until the Status LED turns amber.

Default Settings on the Express Setup Page

Table 2-1 lists the default settings for the settings on the Express Setup page.

Table 2-1 Default Settings on the Express Setup Page

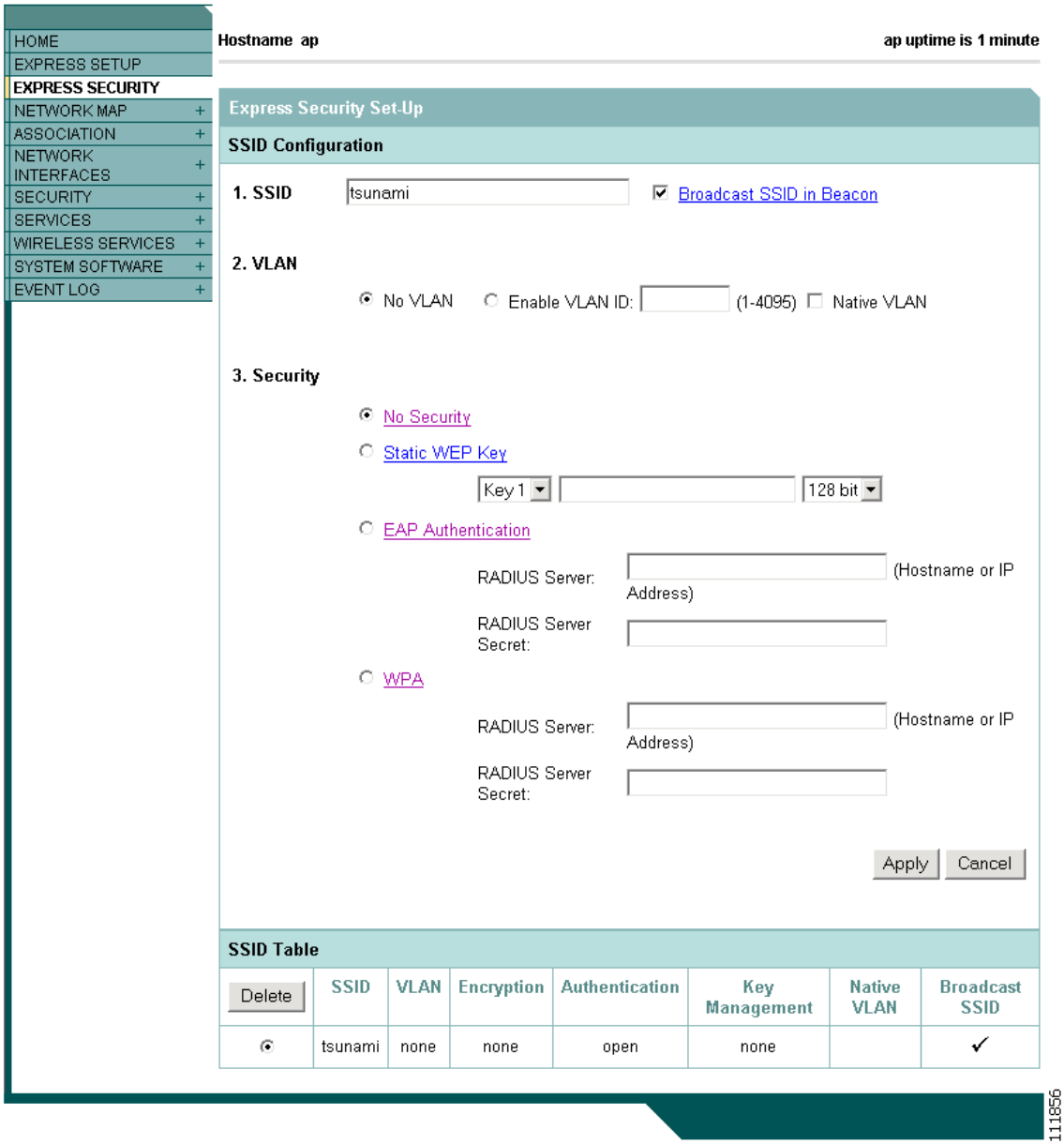
Setting	Default
System Name	ap
Configuration Server Protocol	DHCP
IP Address	Assigned by DHCP by default; if DHCP is disabled, the default setting is 10.0.0.1
IP Subnet Mask	Assigned by DHCP by default; if DHCP is disabled, the default setting is 255.255.255.224
Default Gateway	Assigned by DHCP by default; if DHCP is disabled, the default setting is 0.0.0.0
Role in Radio Network	Access point (root)
Optimize Radio Network for	Throughput
Aironet Extensions	Enable
SNMP Community	defaultCommunity

Configuring Basic Security Settings

After you assign basic settings to your access point, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the access point can communicate beyond the physical boundaries of your worksite.

Just as you use the Express Setup page to assign basic settings, you can use the Express Security page to create unique SSIDs and assign one of four security types to them. Figure 2-6 shows the Express Security page.

Figure 2-6 Express Security Page



The Express Security page helps you configure basic security settings. You can use the web-browser interface's main Security pages to configure more advanced security settings.

Understanding Express Security Settings

When the access point configuration is at factory defaults, the first SSID that you create using the Express security page overwrites the default SSID, *tsunami*, which has no security settings. The SSIDs that you create appear in the SSID table at the bottom of the page. You can create up to 16 SSIDs on the access point. On dual-radio access points, the SSIDs that you create are enabled on both radio interfaces.

Using VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs using any of the four security settings on the Express Security page. However, if you do not use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because on the Express Security page encryption settings and authentication types are linked. Without VLANs, encryption settings (WEP and ciphers) apply to an interface, such as the 2.4-GHz radio, and you cannot use more than one encryption setting on an interface. For example, when you create an SSID with static WEP with VLANs disabled, you cannot create additional SSIDs with WPA authentication because they use different encryption settings. If you find that the security setting for an SSID conflicts with another SSID, you can delete one or more SSIDs to eliminate the conflict.

Express Security Types

Table 2-2 describes the four security types that you can assign to an SSID.

Table 2-2 Security Types on Express Security Setup Page

Security Type	Description	Security Features Enabled
No Security	This is the least secure option. You should use this option only for SSIDs used in a public space and assign it to a VLAN that restricts access to your network.	None.
Static WEP Key	This option is more secure than no security. However, static WEP keys are vulnerable to attack. If you configure this setting, you should consider limiting association to the access point based on MAC address (see the "Using MAC Address ACLs to Block or Allow Client Association to the Access Point" section on page 16-5) or, if your network does not have a RADIUS server, consider using an access point as a local authentication server (see Chapter 8, "Configuring an Access Point as a Local Authenticator").	Mandatory WEP. Client devices cannot associate using this SSID without a WEP key that matches the access point's key.

Table 2-2 Security Types on Express Security Setup Page (continued)

Security Type	Description	Security Features Enabled
EAP Authentication	This option enables 802.1x authentication (such as LEAP, PEAP, EAP-TLS, EAP-GTC, EAP-SIM, and others) and requires you to enter the IP address and shared secret for an authentication server on your network (server authentication port 1645). Because 802.1x authentication provides dynamic encryption keys, you do not need to enter a WEP key.	Mandatory 802.1x authentication. Client devices that associate using this SSID must perform 802.1x authentication.
WPA	Wi-Fi Protected Access (WPA) permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their IP traffic with stronger algorithms than those used in WEP. As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).	Mandatory WPA authentication. Client devices that associate using this SSID must be WPA-capable.

Express Security Limitations

Because the Express Security page is designed for simple configuration of basic security, the options available are a subset of the access point's security capabilities. Keep these limitations in mind when using the Express Security page:

- You cannot edit SSIDs. However, you can delete SSIDs and re-create them.
- You cannot assign SSIDs to specific radio interfaces. The SSIDs that you create are enabled on all radio interfaces. To assign SSIDs to specific radio interfaces, use the Security SSID Manager page.
- You cannot configure multiple authentication servers. To configure multiple authentication servers, use the Security Server Manager page.
- You cannot configure multiple WEP keys. To configure multiple WEP keys, use the Security Encryption Manager page.
- You cannot assign an SSID to a VLAN that is already configured on the access point. To assign an SSID to an existing VLAN, use the Security SSID Manager page.
- You cannot configure combinations of authentication types on the same SSID (for example, MAC address authentication and EAP authentication). To configure combinations of authentication types, use the Security SSID Manager page.

Using the Express Security Page

Follow these steps to create an SSID using the Express Security page:

Step 1 Type the SSID in the SSID entry field. The SSID can contain up to 32 alphanumeric characters.

Step 2 To broadcast the SSID in the access point beacon, check the Broadcast SSID in Beacon check box. When you broadcast the SSID, devices that do not specify an SSID can associate to the access point. This is a useful option for an SSID used by guests or by client devices in a public space. If you do not broadcast the SSID, client devices cannot associate to the access point unless their SSID matches this SSID. Only one SSID can be included in the access point beacon.

Step 3 (Optional) Check the Enable VLAN ID check box and enter a VLAN number (1 through 4095) to assign the SSID to a VLAN. You cannot assign an SSID to an existing VLAN.

Step 4 (Optional) Check the Native VLAN check box to mark the VLAN as the native VLAN.

Step 5 Select the security setting for the SSID. The settings are listed in order of robustness, from No Security to WPA, which is the most secure setting. If you select EAP Authentication or WPA, enter the IP address and shared secret for the authentication server on your network.

Note If you do not use VLANs on your wireless LAN, the security options that you can assign to multiple SSIDs are limited. See the "Using VLANs" section on page 2-12 for details.

Step 6 Click **Apply**. The SSID appears in the SSID table at the bottom of the page.

CLI Configuration Examples

The examples in this section show the CLI commands that are equivalent to creating SSIDs using each security type on the Express Security page. This section contains these example configurations:

- Example: No Security, page 2-14
- Example: Static WEP, page 2-15
- Example: EAP Authentication, page 2-16
- Example: WPA, page 2-18

Example: No Security

This example shows part of the configuration that results from using the Express Security page to create an SSID called *no_security_ssid*, including the SSID in the beacon, assigning it to VLAN 10, and selecting VLAN 10 as the native VLAN:

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid no_security_ssid
    vlan 10
    authentication open
    guest-mode
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
```

```
 station-role root
!
interface Dot11Radio0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 ssid no_security_ssid
    vlan 10
    authentication open
    guest-mode
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 station-role root
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
```

Example: Static WEP

This example shows part of the configuration that results from using the Express Security page to create an SSID called *static_wep_ssid*, excluding the SSID from the beacon, assigning the SSID to VLAN 20, selecting 3 as the key slot, and entering a 128-bit key:

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 20 key 3 size 128bit 7 FFD518A21653687A4251AEE1230C transmit-key
 encryption vlan 20 mode wep mandatory
 !
 ssid static_wep_ssid
    vlan 20
    authentication open
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
```

```
interface Dot11Radio0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
 bridge-group 20 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption vlan 20 key 3 size 128bit 7 741F07447BA1D4382450CB68F37A transmit-key
 encryption vlan 20 mode wep mandatory
 !
 ssid static_wep_ssid
    vlan 20
    authentication open
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
 bridge-group 20 spanning-disabled
```

Example: EAP Authentication

This example shows part of the configuration that results from using the Express Security page to create an SSID called *eap_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 30:

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 30 mode wep mandatory
 !
 ssid eap_ssid
    vlan 30
    authentication open eap eap_methods
    authentication network-eap eap_methods
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
```

```
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption vlan 30 mode wep mandatory
 !
 ssid eap_ssid
    vlan 30
    authentication open eap eap_methods
    authentication network-eap eap_methods
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
interface FastEthernet0
 mtu 1500
 no ip address
 ip mtu 1564
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.30
 mtu 1500
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 no bridge-group 30 source-learning
 bridge-group 30 spanning-disabled
```

```
!
interface BVI1
 ip address 10.91.104.91 255.255.255.192
 no ip route-cache
!
ip http server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip radius source-interface BVI1
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.91.104.92 auth-port 1645 acct-port 1646 key 7 091D1C5A4D5041
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
```

Example: WPA

This example shows part of the configuration that results from using the Express Security page to create an SSID called *wpa_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 40:

```
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.91.104.92 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 40 mode ciphers tkip
 !
 ssid wpa_ssid
    vlan 40
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
```

```
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
 bridge-group 40 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 no bridge-group 40 source-learning
 bridge-group 40 spanning-disabled
```

Using the IP Setup Utility

IPSU enables you to find the access point's IP address when it has been assigned by a DHCP server. You can also use IPSU to set the access point's IP address and SSID if they have not been changed from the default settings. This section explains how to install the utility, how to use it to find the access point's IP address, and how to use it to set the IP address and the SSID.

Note IPSU can be used only on the following operating systems: Windows 95, 98, NT, 2000, ME, or XP.

Tip Another simple way to find the access point's IP address is to look on the Status screen in the Aironet Client Utility on a client device associated to the access point.

Obtaining IPSU

IPSU is available on the Cisco web site. Click this link to browse to the Software Center on Cisco.com:

http://www.cisco.com/public/sw-center/sw-wireless.shtml

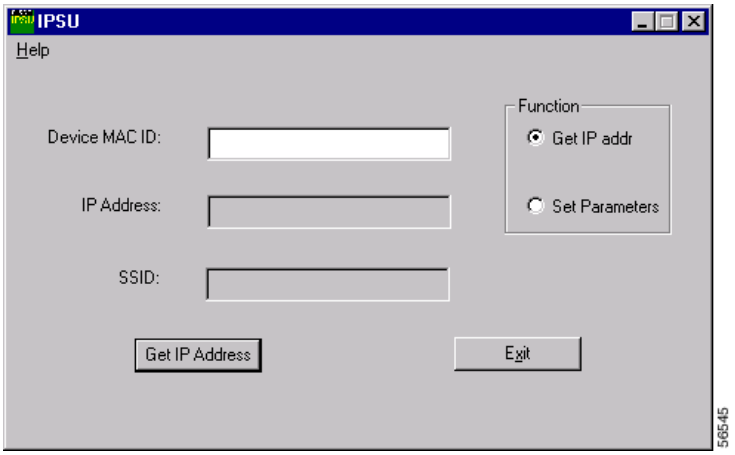
You can find IPSU in the Software Display Tables for access points that run Cisco IOS software.

Using IPSU to Find the Access Point's IP Address

If your access point receives an IP address from a DHCP server, you can use IPSU to find its IP address. Because IPSU sends a reverse-ARP request based on the access point MAC address, you must run IPSU from a computer on the same subnet as the access point. Follow these steps to find the access point's IP address:

Step 1 Double-click the **IPSU** icon on your computer desktop to start the utility. The IPSU screen appears (see Figure 2-7).

Figure 2-7 IPSU Get IP Address Screen



Step 2 When the utility window opens, make sure the *Get IP addr* radio button in the Function box is selected.

Step 3 Enter the access point's MAC address in the Device MAC ID field. The access point's MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your access point's MAC address might look like the following example:

000164xxxxxx

Note The MAC address field is not case-sensitive.

Step 4 Click **Get IP Address**.

Step 5 When the access point's IP address appears in the IP Address field, write it down.

If IPSU reports that the IP address is 10.0.0.1, the default IP address, then the access point did not receive a DHCP-assigned IP address. To change the access point IP address from the default value using IPSU, refer to the "Using IPSU to Set the Access Point's IP Address and SSID" section on page 2-21.

Using IPSU to Set the Access Point's IP Address and SSID

If you want to change the default IP address (10.0.0.1) of the access point, you can use IPSU. You can also set the access point's SSID at the same time.

Note IPSU can change the access point's IP address and SSID only from their default settings. After the IP address and SSID have been changed, IPSU cannot change them again.

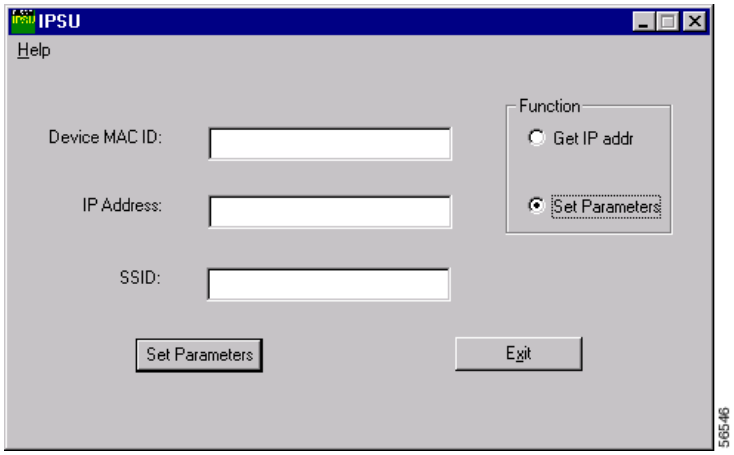
Note The computer you use to assign an IP address to the access point must have an IP address in the same subnet as the access point (10.0.0.x).

Follow these steps to assign an IP address and an SSID to the access point:

Step 1 Double-click the **IPSU** icon on your computer desktop to start the utility.

Step 2 Click the **Set Parameters** radio button in the Function box (see Figure 2-8).

Figure 2-8 IPSU Set Parameters Screen



Step 3 Enter the access point's MAC address in the Device MAC ID field. The access point's MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your access point's MAC address might look like this example:

004096xxxxxx

Note The MAC address field is not case-sensitive.

Step 4 Enter the IP address you want to assign to the access point in the IP Address field.

Step 5 Enter the SSID you want to assign to the access point in the SSID field.

Note You cannot set the SSID without also setting the IP address. However, you can set the IP address without setting the SSID.

Step 6 Click **Set Parameters** to change the access point's IP address and SSID settings.

Step 7 Click **Exit** to exit IPSU.

Assigning an IP Address Using the CLI

When you connect the access point to the wired LAN, the access point links to the network using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the access point's Ethernet and radio ports, the network uses the BVI.

When you assign an IP address to the access point using the CLI, you must assign the address to the BVI. Beginning in privileged EXEC mode, follow these steps to assign an IP address to the access point's BVI:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface bvi1**	Enter interface configuration mode for the BVI.
Step 3	**ip address** *address mask*	Assign an IP address and address mask to the BVI. **Note** If you are connected to the access point using a Telnet session, you lose your connection to the access point when you assign a new IP address to the BVI. If you need to continue configuring the access point using Telnet, use the new IP address to open another Telnet session to the access point.

Using a Telnet Session to Access the CLI

Follow these steps to browse to access the CLI using a Telnet session. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start > Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

Step 2 When the Telnet window appears, click **Connect** and select **Remote System**.

Note In Windows 2000, the Telnet window does not contain drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the access point's IP address.

Step 3 In the Host Name field, type the access point's IP address and click **Connect**.

CHAPTER 3

Using the Web-Browser Interface

This chapter describes the web-browser interface that you can use to configure the access point. It contains these sections:

- Using the Web-Browser Interface for the First Time, page 3-2
- Using the Management Pages in the Web-Browser Interface, page 3-2
- Using Online Help, page 3-5

The web-browser interface contains management pages that you use to change access point settings, upgrade firmware, and monitor and configure other wireless devices on the network.

Note The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

Note Avoid using both the CLI and the web-browser interfaces to configure the access point. If you configure your access point using the CLI, the web-browser interface might display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the access point is misconfigured.

Using the Web-Browser Interface for the First Time

Use the access point's IP address to browse to the management system. See the "Obtaining and Assigning an IP Address" section on page 2-3 for instructions on assigning an IP address to the access point.

Follow these steps to begin using the web-browser interface:

Step 1 Start the browser.

Step 2 Enter the access point's IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer) and press **Enter**. The Summary Status page appears.

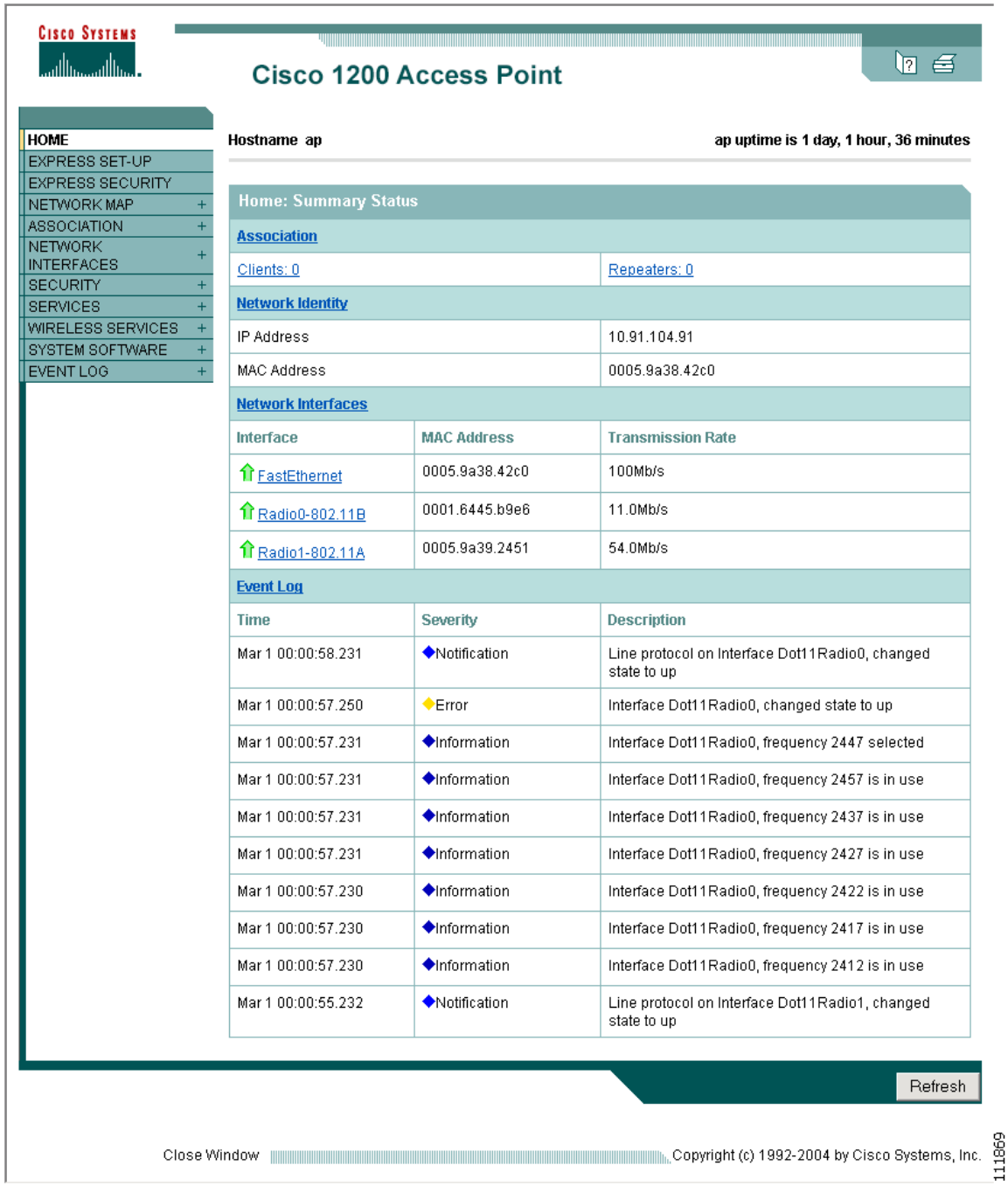
Using the Management Pages in the Web-Browser Interface

The system management pages use consistent techniques to present and save configuration information. A navigation bar is on the left side of the page, and configuration action buttons appear at the bottom. You use the navigation bar to browse to other management pages, and you use the configuration action buttons to save or cancel changes to the configuration.

Note It's important to remember that clicking your browser's **Back** button returns you to the previous page without saving any changes you have made. Clicking **Cancel** cancels any changes you made on the page and keeps you on that page. Changes are only applied when you click **Apply**.

Figure 3-1 shows the web-browser interface home page.

Figure 3-1 Web-Browser Interface Home Page


Cisco Systems
Cisco 1200 Access Point
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +
Hostname ap
ap uptime is 1 day, 1 hour, 36 minutes
Home: Summary Status
Association
Clients: 0
Repeaters: 0
Network Identity
IP Address 10.91.104.91
MAC Address 0005.9a38.42c0
Network Interfaces
Interface MAC Address Transmission Rate
FastEthernet 0005.9a38.42c0 100Mb/s
Radio0-802.11B 0001.6445.b9e6 11.0Mb/s
Radio1-802.11A 0005.9a39.2451 54.0Mb/s
Event Log
Time Severity Description
Mar 1 00:00:58.231 Notification Line protocol on Interface Dot11Radio0, changed state to up
Mar 1 00:00:57.250 Error Interface Dot11Radio0, changed state to up
Mar 1 00:00:57.231 Information Interface Dot11Radio0, frequency 2447 selected
Mar 1 00:00:57.231 Information Interface Dot11Radio0, frequency 2457 is in use
Mar 1 00:00:57.231 Information Interface Dot11Radio0, frequency 2437 is in use
Mar 1 00:00:57.231 Information Interface Dot11Radio0, frequency 2427 is in use
Mar 1 00:00:57.230 Information Interface Dot11Radio0, frequency 2422 is in use
Mar 1 00:00:57.230 Information Interface Dot11Radio0, frequency 2417 is in use
Mar 1 00:00:57.230 Information Interface Dot11Radio0, frequency 2412 is in use
Mar 1 00:00:55.232 Notification Line protocol on Interface Dot11Radio1, changed state to up
Refresh
Close Window
Copyright (c) 1992-2004 by Cisco Systems, Inc.
111869

Using Action Buttons

Table 3-1 lists the page links and buttons that appear on most management pages.

Table 3-1 Common Buttons on Management Pages

Button/Link	Description
Navigation Links	
Home	Displays access point status page with information on the number of radio devices associated to the access point, the status of the Ethernet and radio interfaces, and a list of recent access point activity.
Express Setup	Displays the Express Setup page that includes basic settings such as system name, IP address, and role in radio network.
Express Security	Displays the Express Security page that you use to create SSID and assign security settings to them.
Network Map	Displays a list of infrastructure devices on your wireless LAN.
Association	Displays a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships.
Network Interfaces	Displays status and statistics for the Ethernet and radio interfaces and provides links to configuration pages for each interface.
Security	Displays a summary of security settings and provides links to security configuration pages.
Services	Displays status for several access point features and links to configuration pages for Telnet/SSH, CDP, domain name server, filters, proxy Mobile IP, QoS, SNMP, SNTP, and VLANs.
Wireless Services	Displays a summary of wireless services used with CCKM and provides links to WDS configuration pages.
System Software	Displays the version number of the firmware that the access point is running and provides links to configuration pages for upgrading and managing firmware.
Event Log	Displays the access point event log and provides links to configuration pages where you can select events to be included in traps, set event severity levels, and set notification methods.
Configuration Action Buttons	
Apply	Saves changes made on the page and remains on the page.
Refresh	Updates status information or statistics displayed on a page.
Cancel	Discards changes to the page and remains on the page.
Back	Discards any changes made to the page and returns to the previous page.

Character Restrictions in Entry Fields

Because the 1200 series access point uses Cisco IOS software, there are certain characters that you cannot use in the entry fields on the web-browser interface. Table 3-2 lists the illegal characters and the fields in which you cannot use them.

Table 3-2 Illegal Characters for Web-Browser Interface Entry Fields

Entry Field Type	Illegal Characters
Password entry fields	**?** **“** **$** **[** **+**
All other entry fields	**?** **“** **$** **[** **+** You also cannot use these three characters as the first character in an entry field: **!** **#** **;**

Using Online Help

Click the help icon at the top of any page in the web-browser interface to display online help. Figure 3-2 shows the help and print icons.

Figure 3-2 Help and Print Icons

When a help page appears in a new browser window, use the Select a topic drop-down menu to display the help index or instructions for common configuration tasks, such as configuring VLANs.

Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) that you can use to configure your access point. It contains these sections:

- Cisco IOS Command Modes, page 4-2
- Getting Help, page 4-3
- Abbreviating Commands, page 4-3
- Using no and default Forms of Commands, page 4-3
- Understanding CLI Messages, page 4-4
- Using Command History, page 4-4
- Using Editing Features, page 4-5
- Searching and Filtering Output of show and more Commands, page 4-8
- Accessing the CLI, page 4-8

Cisco IOS Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the access point, you begin in user mode, often called *user EXEC mode*. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the access point reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you must enter privileged EXEC mode before you can enter the global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the access point reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

Table 4-1 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name *ap*.

Table 4-1 Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your access point.	`ap>`	Enter **logout** or **quit**.	Use this mode to: • Change terminal settings • Perform basic tests • Display system information
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`ap#`	Enter **disable** to exit.	Use this mode to verify commands. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`ap(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire access point.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`ap(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet and radio interfaces. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

Getting Help

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command, as shown in Table 4-2.

Table 4-2 Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.

*abbreviated-command-entry***?**	Obtains a list of commands that begin with a particular character string.
	For example:
	`ap# di?`
	`dir  disable  disconnect`

abbreviated-command-entry<**Tab**>	Completes a partial command name.
	For example:
	`ap# sh conf<tab>`
	`ap# show configuration`

?	Lists all commands available for a particular command mode. For example: `ap> ?`
command **?**	Lists the associated keywords for a command. For example: `ap> show ?`

command keyword **?**	Lists the associated arguments for a keyword.
	For example:
	`ap(config)# cdp holdtime ?`
	`  <10-255>  Length of time (in sec) that receiver must keep this packet`

Abbreviating Commands

You have to enter only enough characters for the access point to recognize the command as unique. This example shows how to enter the **show configuration** privileged EXEC command:

```
ap# show conf
```

Using no and default Forms of Commands

Most configuration commands also have a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

Understanding CLI Messages

Table 4-3 lists some error messages that you might encounter while using the CLI to configure your access point.

Table 4-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your access point to recognize the command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (**?**) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command are displayed.

Using Command History

The CLI provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize the command history feature to suit your needs as described in these sections:

- Changing the Command History Buffer Size, page 4-4
- Recalling Commands, page 4-5
- Disabling the Command History Feature, page 4-5

Changing the Command History Buffer Size

By default, the access point records ten command lines in its history buffer. Beginning in privileged EXEC mode, enter this command to change the number of command lines that the access point records during the current terminal session:

```
ap# terminal history [size number-of-lines]
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the access point records for all sessions on a particular line:

```
ap(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in Table 4-4:

Table 4-4 Recalling Commands

Action[1]	Result
Press **Ctrl-P** or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that are displayed is determined by the setting of the **terminal history** global configuration command and **history** line configuration command.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disabling the Command History Feature

The command history feature is automatically enabled.

To disable the feature during the current terminal session, enter the **terminal no history** privileged EXEC command.

To disable command history for the line, enter the **no history** line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line. It contains these sections:

- Enabling and Disabling Editing Features, page 4-6
- Editing Commands Through Keystrokes, page 4-6
- Editing Command Lines that Wrap, page 4-7

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it.

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
ap# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# editing
```

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# no editing
```

Editing Commands Through Keystrokes

Table 4-5 shows the keystrokes that you need to edit command lines.

Table 4-5 Editing Commands Through Keystrokes

Capability	Keystroke[1]	Purpose
Move around the command line to make changes or corrections.	**Ctrl-B** or the left arrow key	Move the cursor back one character.
	Ctrl-F or the right arrow key	Move the cursor forward one character.
	Ctrl-A	Move the cursor to the beginning of the command line.
	Ctrl-E	Move the cursor to the end of the command line.
	Esc B	Move the cursor back one word.
	Esc F	Move the cursor forward one word.
	Ctrl-T	Transpose the character to the left of the cursor with the character located at the cursor.
Recall commands from the buffer and paste them in the command line. The access point provides a buffer with the last ten items that you deleted.	**Ctrl-Y**	Recall the most recent entry in the buffer.
	Esc Y	Recall the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	**Delete** or **Backspace**	Erase the character to the left of the cursor.
	Ctrl-D	Delete the character at the cursor.
	Ctrl-K	Delete all characters from the cursor to the end of the command line.
	Ctrl-U or **Ctrl-X**	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W	Delete the word to the left of the cursor.
	Esc D	Delete from the cursor to the end of the word.

Table 4-5 Editing Commands Through Keystrokes (continued)

Capability	Keystroke[1]	Purpose
Capitalize or lowercase words or capitalize a set of letters.	**Esc C**	Capitalize at the cursor.
	Esc L	Change the word at the cursor to lowercase.
	Esc U	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	**Ctrl-V** or **Esc Q**	
Scroll down a line or screen on displays that are longer than the terminal screen can display. **Note** The `More` prompt appears for output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the `More` prompt.	**Return**	Scroll down one line.
	Space	Scroll down one screen.
Redisplay the current command line if the access point suddenly sends a message to your screen.	**Ctrl-L** or **Ctrl-R**	Redisplay the current command line.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Editing Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
ap(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
ap(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
ap(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see the "Editing Commands Through Keystrokes" section on page 4-6.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the *pipe* character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

command **|** {**begin** | **include** | **exclude**} *regular-expression*

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
ap# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

Accessing the CLI

You can open the access point's CLI using Telnet or Secure Shell (SSH).

Opening the CLI with Telnet

Follow these steps to open the CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start > Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

Step 2 When the Telnet window appears, click **Connect** and select **Remote System**.

Note In Windows 2000, the Telnet window does not contain drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the access point's IP address.

Step 3 In the Host Name field, type the access point's IP address and click **Connect**.

Step 4 At the username and password prompts, enter your administrator username and password. The default username is **Cisco**, and the default password is **Cisco**. The default enable password is also **Cisco**. Usernames and passwords are case-sensitive.

Opening the CLI with Secure Shell

Secure Shell Protocol is a protocol that provides a secure, remote connection to networking devices set up to use it. Secure Shell (SSH) is a software package that provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection. For detailed information on SSH, visit the homepage of SSH Communications Security, Ltd. at this URL: http://www.ssh.com/

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. See the "Configuring the Access Point for Secure Shell" section on page 5-20 for detailed instructions on setting up the access point for SSH access.

CHAPTER 5

Administering the Access Point

This chapter describes how to administer your access point. This chapter contains these sections:

- Preventing Unauthorized Access to Your Access Point, page 5-2
- Protecting Access to Privileged EXEC Commands, page 5-2
- Controlling Access Point Access with RADIUS, page 5-7
- Controlling Access Point Access with TACACS+, page 5-12
- Configuring Ethernet Speed and Duplex Settings, page 5-15
- Configuring the Access Point for Wireless Network Management, page 5-16
- Configuring the Access Point for Local Authentication and Authorization, page 5-16
- Configuring the Access Point to Provide DHCP Service, page 5-18
- Configuring the Access Point for Secure Shell, page 5-20
- Configuring Client ARP Caching, page 5-21
- Managing the System Time and Date, page 5-22
- Configuring a System Name and Prompt, page 5-37
- Creating a Banner, page 5-40

Preventing Unauthorized Access to Your Access Point

You can prevent unauthorized users from reconfiguring your access point and viewing configuration information. Typically, you want network administrators to have access to the access point while you restrict access to users who connect through a terminal or workstation from within the local network.

To prevent unauthorized access to your access point, you should configure one of these security features:

- Username and password pairs, which are locally stored on the access point. These pairs authenticate each user before that user can access the access point. You can also assign a specific privilege level (read only or read/write) to each username and password pair. For more information, see the "Configuring Username and Password Pairs" section on page 5-5. The default username is *Cisco*, and the default password is *Cisco*. Usernames and passwords are case-sensitive.
- Username and password pairs stored centrally in a database on a security server. For more information, see the "Controlling Access Point Access with RADIUS" section on page 5-7.

Protecting Access to Privileged EXEC Commands

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can issue after they have logged into a network device.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

This section describes how to control access to the configuration file and privileged EXEC commands. It contains this configuration information:

- Default Password and Privilege Level Configuration, page 5-2
- Setting or Changing a Static Enable Password, page 5-3
- Protecting Enable and Enable Secret Passwords with Encryption, page 5-4
- Configuring Username and Password Pairs, page 5-5
- Configuring Multiple Privilege Levels, page 5-6

Default Password and Privilege Level Configuration

Table 5-1 shows the default password and privilege level configuration.

Table 5-1 Default Password and Privilege Levels

Feature	Default Setting
Username and password	Default username is *Cisco* and the default password is *Cisco.*
Enable password and privilege level	Default password is *Cisco*. The default is level 15 (privileged EXEC level). The password is encrypted in the configuration file.

Table 5-1 Default Password and Privilege Levels (continued)

Feature	Default Setting
Enable secret password and privilege level	The default enable password is *Cisco*. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	Default password is *Cisco*. The password is encrypted in the configuration file.

Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode.

Note The **no enable password** global configuration command removes the enable password, but you should use extreme care when using this command. If you remove the enable password, you are locked out of the EXEC mode.

Beginning in privileged EXEC mode, follow these steps to set or change a static enable password:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**enable password** *password*	Define a new password or change an existing password for access to privileged EXEC mode. The default password is *Cisco*. For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Crtl-V when you create the password; for example, to create the password abc?123, do this: 1. Enter **abc**. 2. Enter **Crtl-V**. 3. Enter **?123**. When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-V; you can simply enter abc?123 at the password prompt.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file. The enable password is not encrypted and can be read in the access point configuration file.

This example shows how to change the enable password to *l1u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
AP(config)# enable password l1u2c3k4y5
```

Protecting Enable and Enable Secret Passwords with Encryption

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use either the **enable password** or **enable secret** global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

Cisco recommends that you use the **enable secret** command because it uses an improved encryption algorithm.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable and enable secret passwords:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}	Define a new password or change an existing password for access to privileged EXEC mode.
	or	or
	enable secret [**level** *level*] {*password* | *encryption-type encrypted-password*}	Define a secret password, which is saved using a nonreversible encryption method. • (Optional) For *level*, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges). • For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. • (Optional) For *encryption-type*, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password you copy from another access point configuration. **Note** If you specify an encryption type and then enter a clear text password, you can not re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.
Step 3	**service password-encryption**	(Optional) Encrypt the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

If both the enable and enable secret passwords are defined, users must enter the enable secret password.

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels. For more information, see the "Configuring Multiple Privilege Levels" section on page 5-6.

If you enable password encryption, it applies to all passwords including username passwords, authentication key passwords, the privileged command password, and console and virtual terminal line passwords.

To remove a password and level, use the **no enable password** [**level** *level*] or **no enable secret** [**level** *level*] global configuration command. To disable password encryption, use the **no service password-encryption** global configuration command.

This example shows how to configure the encrypted password *1FaD0$Xyti5Rkls3LoyxzS8* for privilege level 2:

```
AP(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Configuring Username and Password Pairs

You can configure username and password pairs, which are locally stored on the access point. These pairs are assigned to lines or interfaces and authenticate each user before that user can access the access point. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	Enter the username, privilege level, and password for each user. • For *name*, specify the user ID as one word. Spaces and quotation marks are not allowed. • (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access. • For *encryption-type*, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow. • For *password*, specify the password the user must enter to gain access to the access point. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
Step 3	**login local**	Enable local password checking at login time. Authentication is based on the username specified in Step 2.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable username authentication for a specific user, use the **no username** *name* global configuration command.

To disable password checking and allow connections without a password, use the **no login** line configuration command.

Note You must have at least one username configured and you must have login local set to open a Telnet session to the access point. If you enter no username for the only username, you can be locked out of the access point.

Configuring Multiple Privilege Levels

By default, Cisco IOS software has two modes of password security: user EXEC and privileged EXEC. You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

For example, if you want many users to have access to the **clear line** command, you can assign it level 2 security and distribute the level 2 password fairly widely. But if you want more restricted access to the **configure** command, you can assign it level 3 security and distribute that password to a more restricted group of users.

This section includes this configuration information:

- Setting the Privilege Level for a Command, page 5-6
- Logging Into and Exiting a Privilege Level, page 5-7

Setting the Privilege Level for a Command

Beginning in privileged EXEC mode, follow these steps to set the privilege level for a command mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**privilege** *mode* **level** *level command*	Set the privilege level for a command. • For *mode*, enter **configure** for global configuration mode, **exec** for EXEC mode, **interface** for interface configuration mode, or **line** for line configuration mode. • For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password. • For *command*, specify the command to which you want to restrict access.
Step 3	**enable password level** *level password*	Specify the enable password for the privilege level. • For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. • For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.

	Command	Purpose
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config** or **show privilege**	Verify your entries. The first command displays the password and access level configuration. The second command displays the privilege level configuration.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15 unless you set them individually to different levels.

To return to the default privilege for a given command, use the **no privilege** *mode* **level** *level command* global configuration command.

This example shows how to set the **configure** command to privilege level 14 and define *SecretPswd14* as the password users must enter to use level 14 commands:

```
AP(config)# privilege exec level 14 configure
AP(config)# enable password level 14 SecretPswd14
```

Logging Into and Exiting a Privilege Level

Beginning in privileged EXEC mode, follow these steps to log in to a specified privilege level and to exit to a specified privilege level:

	Command	Purpose
Step 1	**enable** *level*	Log in to a specified privilege level. For *level*, the range is 0 to 15.
Step 2	**disable** *level*	Exit to a specified privilege level. For *level*, the range is 0 to 15.

Controlling Access Point Access with RADIUS

This section describes how to control administrator access to the access point using Remote Authentication Dial-In User Service (RADIUS). For complete instructions on configuring the access point to support RADIUS, see Chapter 12, "Configuring RADIUS and TACACS+ Servers."

RADIUS provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS is facilitated through AAA and can be enabled only through AAA commands.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

These sections describe RADIUS configuration:

- Default RADIUS Configuration, page 5-8
- Configuring RADIUS Login Authentication, page 5-8 (required)
- Defining AAA Server Groups, page 5-9 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 5-11 (optional)
- Displaying the RADIUS Configuration, page 5-12

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the access point through the CLI.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **local**—Use the local username database for authentication. You must enter username information in the database. Use the **username** *password* global configuration command. • **radius**—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the "Identifying the RADIUS Server Host" section on page 12-4.
Step 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	**login authentication** {**default** | *list-name*}	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** {**default** \| *list-name*} line configuration command.

Defining AAA Server Groups

You can configure the access point to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	Specify the IP address or host name of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.

	Command	Purpose
Step 4	**aaa group server radius** *group-name*	Define the AAA server-group with a group name. This command puts the access point in a server group configuration mode.
Step 5	**server** *ip-address*	Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.
Step 9		Enable RADIUS login authentication. See the "Configuring RADIUS Login Authentication" section on page 5-8.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server** *ip-address* server group configuration command.

In this example, the access point is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the access point uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa authorization network radius**	Configure the access point for user RADIUS authorization for all network-related service requests.
Step 3	**aaa authorization exec radius**	Configure the access point for user RADIUS authorization to determine if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** privileged EXEC command.

Controlling Access Point Access with TACACS+

This section describes how to control administrator access to the access point using Terminal Access Controller Access Control System Plus (TACACS+). For complete instructions on configuring the access point to support TACACS+, see Chapter 12, "Configuring RADIUS and TACACS+ Servers."

TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

These sections describe TACACS+ configuration:

- Default TACACS+ Configuration, page 5-13
- Configuring TACACS+ Login Authentication, page 5-13
- Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 5-14
- Displaying the TACACS+ Configuration, page 5-15

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application.When enabled, TACACS+ can authenticate administrators accessing the access point through the CLI.

Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **local**—Use the local username database for authentication. You must enter username information into the database. Use the **username** *password* global configuration command. • **tacacs+**—Use TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.
Step 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	**login authentication** {**default** | *list-name*}	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] global configuration command. To either disable TACACS+ authentication for logins or to return to the default value, use the **no login authentication** {**default** \| *list-name*} line configuration command.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the access point uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa authorization network tacacs+**	Configure the access point for user TACACS+ authorization for all network-related service requests.
Step 3	**aaa authorization exec tacacs+**	Configure the access point for user TACACS+ authorization to determine if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the **show tacacs** privileged EXEC command.

Configuring Ethernet Speed and Duplex Settings

You can assign the access point Ethernet port speed and duplex settings. Cisco recommends that you use **auto**, the default setting, for both the speed and duplex settings on the access point Ethernet port. When your access point receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the access point. If the switch port to which the access point is connected is not set to **auto**, you can change the access point port to **half** or **full** to correct a duplex mismatch and the Ethernet link is not reset. However, if you change from **half** or **full** back to **auto**, the link is reset and, if your access point receives inline power from a switch, the access point reboots.

Note The speed and duplex settings on the access point Ethernet port must match the Ethernet settings on the port to which the access point is connected. If you change the settings on the port to which the access point is connected, change the settings on the access point Ethernet port to match.

The Ethernet speed and duplex are set to **auto** by default. Beginning in privileged EXEC mode, follow these steps to configure Ethernet speed and duplex:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface fastethernet0**	Enter configuration interface mode.
Step 3	**speed** { **10** | **100** | **auto** }	Configure the Ethernet speed. Cisco recommends that you use **auto**, the default setting.
Step 4	**duplex** { **auto** | **full** | **half** }	Configure the duplex setting. Cisco recommends that you use **auto**, the default setting.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring the Access Point for Wireless Network Management

You can enable the access point for wireless network management. The wireless network manager (WNM) manages the devices on your wireless LAN.

Enter this command to configure the access point to interact with the WNM:

```
AP(config)# wlccp wnm ip address ip-address
```

Enter this command to check the authentication status between the WDS access point and the WNM:

```
AP# show wlccp wnm status
```

Possible statuses are *not authenticated*, *authentication in progress*, *authentication fail*, *authenticated*, and *security keys setup*.

Configuring the Access Point for Local Authentication and Authorization

You can configure AAA to operate without a server by configuring the access point to implement AAA in local mode. The access point then handles authentication and authorization. No accounting is available in this configuration.

Note You can configure your access point as a local authenticator for 802.1x-enabled client devices to provide a backup for your main server or to provide authentication service on a network without a RADIUS server. See Chapter 8, "Configuring an Access Point as a Local Authenticator," for detailed instructions on configuring your access point as a local authenticator.

Beginning in privileged EXEC mode, follow these steps to configure the access point for local AAA:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**aaa authentication login default local**	Set the login authentication to use the local username database. The **default** keyword applies the local user database authentication to all interfaces.
Step 4	**aaa authorization exec local**	Configure user AAA authorization to determine if the user is allowed to run an EXEC shell by checking the local database.
Step 5	**aaa authorization network local**	Configure user AAA authorization for all network-related service requests.
Step 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	Enter the local database, and establish a username-based authentication system. Repeat this command for each user. • For *name*, specify the user ID as one word. Spaces and quotation marks are not allowed. • (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access. • For *encryption-type*, enter **0** to specify that an unencrypted password follows. Enter **7** to specify that a hidden password follows. • For *password*, specify the password the user must enter to gain access to the access point. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Configuring the Access Point to Provide DHCP Service

These sections describe how to configure the access point to act as a DHCP server:

- Setting up the DHCP Server, page 5-18
- Monitoring and Maintaining the DHCP Server Access Point, page 5-19

Setting up the DHCP Server

By default, access points are configured to receive IP settings from a DHCP server on your network. You can also configure an access point to act as a DHCP server to assign IP settings to devices on both your wired and wireless LANs.

The 1100 series access point becomes a mini-DHCP server by default when it is configured with factory default settings and it cannot receive IP settings from a DHCP server. As a mini-DHCP server, the 1100 series access point provides up to 20 IP addresses between 10.0.0.11 and 10.0.0.30 to a PC connected to its Ethernet port and to wireless client devices configured to use either no SSID or *tsunami* as the SSID, and with all security settings disabled. The mini-DHCP server feature is disabled automatically when you assign a static IP address to the 1100 series access point. Because it has a console port to simplify initial setup, the 1200 series access point does not become a DHCP server automatically.

For detailed information on DHCP-related commands and options, refer to the Configuring DHCP chapter in the *Cisco IOS IP Configuration Guide, Release 12.2*. Click this URL to browse to the "Configuring DHCP" chapter:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

Beginning in privileged EXEC mode, follow these steps to configure an access point to provide DHCP service:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip dhcp excluded-address** *low_address* [*high_address*]	Exclude the access point's IP address from the range of addresses the access point assigns. Enter the IP address in four groups of characters, such as 10.91.6.158. The access point assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP Server should not assign to clients. (Optional) To enter a range of excluded addresses, enter the address at the low end of the range followed by the address at the high end of the range.
Step 3	**ip dhcp pool** *pool_name*	Create a name for the pool of IP addresses that the access point assigns in response to DHCP requests, and enter DHCP configuration mode.
Step 4	**network** *subnet_number* [*mask* | *prefix-length*]	Assign the subnet number for the address pool. The access point assigns IP addresses within this subnet. (Optional) Assign a subnet mask for the address pool, or specify the number of bits that comprise the address prefix. The prefix is an alternative way of assigning the network mask. The prefix length must be preceded by a forward slash (/).

	Command	Purpose
Step 5	**lease** { *days* [*hours*] [*minutes*] | **infinite** }	Configure the duration of the lease for IP addresses assigned by the access point. • days—configure the lease duration in number of days • (optional) hours—configure the lease duration in number of hours • (optional) minutes—configure the lease duration in number of minutes • infinite—set the lease duration to infinite
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of these commands to return to default settings.

This example shows how to configure the access point as a DHCP server:

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.117
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# end
```

Monitoring and Maintaining the DHCP Server Access Point

These sections describe commands you can use to monitor and maintain the DHCP server access point:

- Show Commands, page 5-19
- Clear Commands, page 5-20
- Debug Command, page 5-20

Show Commands

In Exec mode, enter the commands in Table 5-2 to display information about the access point as DHCP server.

Table 5-2 Show Commands for DHCP Server

Command	Purpose
show ip dhcp conflict [*address*]	Displays a list of all address conflicts recorded by a specific DHCP Server. Enter the access point's IP address to show conflicts recorded by the access point.

Table 5-2 Show Commands for DHCP Server (continued)

Command	Purpose
show ip dhcp database [*url*]	Displays recent activity on the DHCP database. **Note** Use this command in privileged EXEC mode.
show ip dhcp server statistics	Displays count information about server statistics and messages sent and received.

Clear Commands

In privileged Exec mode, use the commands in Table 5-3 to clear DHCP server variables.

Table 5-3 Clear Commands for DHCP Server

Command	Purpose
clear ip dhcp binding { *address* | * }	Deletes an automatic address binding from the DHCP database. Specifying the address argument clears the automatic binding for a specific (client) IP address. Specifying an asterisk (*) clears all automatic bindings.
clear ip dhcp conflict { *address* | * }	Clears an address conflict from the DHCP database. Specifying the address argument clears the conflict for a specific IP address. Specifying an asterisk (*) clears conflicts for all addresses.
clear ip dhcp server statistics	Resets all DHCP Server counters to 0.

Debug Command

To enable DHCP server debugging, use this command in privileged EXEC mode:

debug ip dhcp server { **events** | **packets** | **linkage** }

Use the **no** form of the command to disable debugging for the access point DHCP server.

Configuring the Access Point for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.

Note For complete syntax and usage information for the commands used in this section, refer to the "Secure Shell Commands" section in the *Cisco IOS Security Command Reference for Release 12.2.*

Understanding SSH

SSH is a protocol that provides a secure, remote connection to a Layer 2 or a Layer 3 device. There are two versions of SSH: SSH version 1 and SSH version 2. This software release supports only SSH version 1.

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. The SSH feature has an SSH server and an SSH integrated client. The client supports these user authentication methods:

- RADIUS (for more information, see the "Controlling Access Point Access with RADIUS" section on page 5-7)
- Local authentication and authorization (for more information, see the "Configuring the Access Point for Local Authentication and Authorization" section on page 5-16)

For more information about SSH, refer to the "Configuring Secure Shell" section in the *Cisco IOS Security Configuration Guide for Release 12.2*.

Note The SSH feature in this software release does not support IP Security (IPSec).

Configuring SSH

Before configuring SSH, download the crypto software image from Cisco.com. For more information, refer to the release notes for this release.

For information about configuring SSH and displaying SSH settings, refer to the "Configuring Secure Shell" section in the *Cisco IOS Security Configuration Guide for Release 12.2*.

Configuring Client ARP Caching

You can configure the access point to maintain an ARP cache for associated client devices. Maintaining an ARP cache on the access point reduces the trafic load on your wireless LAN. ARP caching is disabled by default.

This section contains this information:

- Understanding Client ARP Caching, page 5-21
- Configuring ARP Caching, page 5-22

Understanding Client ARP Caching

ARP caching on the access point reduces the traffic on your wireless LAN by stopping ARP requests for client devices at the access point. Instead of forwarding ARP requests to client devices, the access point responds to requests on behalf of associated client devices.

When ARP caching is disabled, the access point forwards all ARP requests through the radio port to associated clients, and the client to which the ARP request is directed responds. When ARP caching is enabled, the access point responds to ARP requests for associated clients and does not forward requests to clients. When the access point receives an ARP request for an IP address not in the cache, the access point drops the request and does not forward it. In its beacon, the access point includes an information element to alert client devices that they can safely ignore broadcast messages to increase battery life.

Optional ARP Caching

When a non-Cisco client device is associated to an access point and is not passing data, the access point might not know the client's IP address. If this situation occurs frequently on your wireless LAN, you can enable optional ARP caching. When ARP caching is optional, the access point responds on behalf of clients with IP addresses known to the access point but forwards out its radio port any ARP requests addressed to unknown clients. When the access point learns the IP addresses for all associated clients, it drops ARP requests not directed to its associated clients.

Configuring ARP Caching

Beginning in privileged EXEC mode, follow these steps to configure the access point to maintain an ARP cache for associated clients:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 arp-cache** [**optional**]	Enable ARP caching on the access point. • (Optional) Use the **optional** keyword to enable ARP caching only for the client devices whose IP addresses are known to the access point.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure ARP caching on an access point:

```
AP# configure terminal
AP(config)# dot11 arp-cache
AP(config)# end
```

Managing the System Time and Date

You can manage the system time and date on your access point automatically, using the Network Time Protocol (NTP), or manually, by setting the time and date on the access point.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This section contains this configuration information:

- Understanding the System Clock, page 5-23
- Understanding Network Time Protocol, page 5-23
- Configuring NTP, page 5-24
- Configuring Time and Date Manually, page 5-32

Understanding the System Clock

The heart of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- Network Time Protocol
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

The system clock determines time internally based on Universal Time Coordinated (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that the time is correctly displayed for the local time zone.

The system clock keeps track of whether the time is *authoritative* or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed. For configuration information, see the "Configuring Time and Date Manually" section on page 5-32.

Understanding Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access-list-based restriction scheme and an encrypted authentication mechanism.

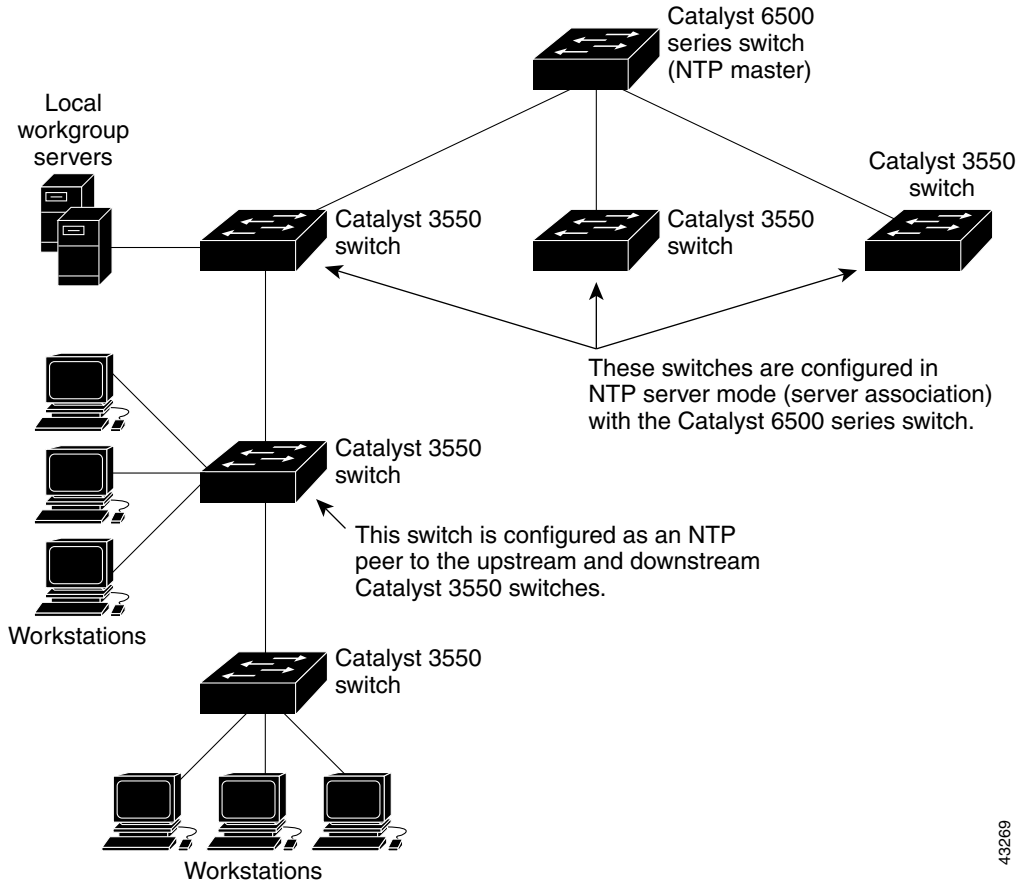
Cisco's implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. Cisco recommends that the time service for your network be derived from the public NTP servers available on the IP Internet. Figure 5-1 shows a typical network example using NTP.

If the network is isolated from the Internet, Cisco's implementation of NTP allows a device to act as though it is synchronized through NTP, when in fact it has determined the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

Figure 5-1 Typical NTP Network Configuration



Configuring NTP

Cisco Aironet 1100 Series Access Points do not have a hardware-supported clock, and they cannot function as an NTP master clock to which peers synchronize themselves when an external NTP source is not available. These access points also have no hardware support for a calendar. As a result, the **ntp update-calendar** and the **ntp master** global configuration commands are not available.

This section contains this configuration information:

- Default NTP Configuration, page 5-25
- Configuring NTP Authentication, page 5-25
- Configuring NTP Associations, page 5-27
- Configuring NTP Broadcast Service, page 5-28
- Configuring NTP Access Restrictions, page 5-29
- Configuring the Source IP Address for NTP Packets, page 5-31
- Displaying the NTP Configuration, page 5-32

Default NTP Configuration

Table 5-4 shows the default NTP configuration.

Table 5-4 Default NTP Configuration

Feature	Default Setting
NTP authentication	Disabled. No authentication key is specified.
NTP peer or server associations	None configured.
NTP broadcast service	Disabled; no interface sends or receives NTP broadcast packets.
NTP access restrictions	No access control is specified.
NTP packet source IP address	The source address is determined by the outgoing interface.

NTP is disabled by default.

Configuring NTP Authentication

This procedure must be coordinated with the administrator of the NTP server; the information you configure in this procedure must be matched by the servers used by the access point to synchronize its time to the NTP server.

Beginning in privileged EXEC mode, follow these steps to authenticate the associations (communications between devices running NTP that provide for accurate timekeeping) with other devices for security purposes:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ntp authenticate**	Enable the NTP authentication feature, which is disabled by default.

	Command	Purpose
Step 3	**ntp authentication-key** *number* **md5** *value*	Define the authentication keys. By default, none are defined. • For *number*, specify a key number. The range is 1 to 4294967295. • **md5** specifies that message authentication support is provided by using the message digest algorithm 5 (MD5). • For *value*, enter an arbitrary string of up to eight characters for the key. The access point does not synchronize to a device unless both have one of these authentication keys, and the key number is specified by the **ntp trusted-key** *key-number* command.
Step 4	**ntp trusted-key** *key-number*	Specify one or more key numbers (defined in Step 3) that a peer NTP device must provide in its NTP packets for this access point to synchronize to it. By default, no trusted keys are defined. For *key-number*, specify the key defined in Step 3. This command provides protection against accidentally synchronizing the access point to a device that is not trusted.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable NTP authentication, use the **no ntp authenticate** global configuration command. To remove an authentication key, use the **no ntp authentication-key** *number* global configuration command. To disable authentication of the identity of a device, use the **no ntp trusted-key** *key-number* global configuration command.

This example shows how to configure the access point to synchronize only to devices providing authentication key 42 in the device's NTP packets:

```
AP(config)# ntp authenticate
AP(config)# ntp authentication-key 42 md5 aNiceKey
AP(config)# ntp trusted-key 42
```

Configuring NTP Associations

An NTP association can be a peer association (this access point can either synchronize to the other device or allow the other device to synchronize to it), or it can be a server association (meaning that only this access point synchronizes to the other device, and not the other way around).

Beginning in privileged EXEC mode, follow these steps to form an NTP association with another device:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ntp peer** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	Configure the access point system clock to synchronize a peer or to be synchronized by a peer (peer association).
	or	or
	ntp server *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	Configure the access point system clock to be synchronized by a time server (server association). No peer or server associations are defined by default. • For *ip-address* in a peer association, specify either the IP address of the peer providing, or being provided, the clock synchronization. For a server association, specify the IP address of the time server providing the clock synchronization. • (Optional) For *number*, specify the NTP version number. The range is 1 to 3. By default, version 3 is selected. • (Optional) For *keyid*, enter the authentication key defined with the **ntp authentication-key** global configuration command. • (Optional) For *interface*, specify the interface from which to pick the IP source address. By default, the source IP address is taken from the outgoing interface. • (Optional) Enter the **prefer** keyword to make this peer or server the preferred one that provides synchronization. This keyword reduces switching back and forth between peers and servers.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

You need to configure only one end of an association; the other device can automatically establish the association. If you are using the default NTP version (version 3) and NTP synchronization does not occur, try using NTP version 2. Many NTP servers on the Internet run version 2.

To remove a peer or server association, use the **no ntp peer** *ip-address* or the **no ntp server** *ip-address* global configuration command.

This example shows how to configure the access point to synchronize its system clock with the clock of the peer at IP address 172.16.22.44 using NTP version 2:

```
AP(config)# ntp server 172.16.22.44 version 2
```

Configuring NTP Broadcast Service

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP addresses of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, the information flow is one-way only.

The access point can send or receive NTP broadcast packets on an interface-by-interface basis if there is an NTP broadcast server, such as a router, broadcasting time information on the network. The access point can send NTP broadcast packets to a peer so that the peer can synchronize to it. The access point can also receive NTP broadcast packets to synchronize its own clock. This section provides procedures for both sending and receiving NTP broadcast packets.

Beginning in privileged EXEC mode, follow these steps to configure the access point to send NTP broadcast packets to peers so that they can synchronize their clock to the access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and specify the interface to send NTP broadcast packets.
Step 3	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]	Enable the interface to send NTP broadcast packets to a peer. By default, this feature is disabled on all interfaces. • (Optional) For *number*, specify the NTP version number. The range is 1 to 3. If you do not specify a version, version 3 is used. • (Optional) For *keyid*, specify the authentication key to use when sending packets to the peer. • (Optional) For *destination-address*, specify the IP address of the peer that is synchronizing its clock to this access point.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.
Step 7		Configure the connected peers to receive NTP broadcast packets as described in the next procedure.

To disable the interface from sending NTP broadcast packets, use the **no ntp broadcast** interface configuration command.

This example shows how to configure an interface to send NTP version 2 packets:

```
AP(config)# interface gigabitethernet0/1
AP(config-if)# ntp broadcast version 2
```

Beginning in privileged EXEC mode, follow these steps to configure the access point to receive NTP broadcast packets from connected peers:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and specify the interface to receive NTP broadcast packets.
Step 3	**ntp broadcast client**	Enable the interface to receive NTP broadcast packets. By default, no interfaces receive NTP broadcast packets.
Step 4	**exit**	Return to global configuration mode.
Step 5	**ntp broadcastdelay** *microseconds*	(Optional) Change the estimated round-trip delay between the access point and the NTP broadcast server. The default is 3000 microseconds; the range is 1 to 999999.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable an interface from receiving NTP broadcast packets, use the **no ntp broadcast client** interface configuration command. To change the estimated round-trip delay to the default, use the **no ntp broadcastdelay** global configuration command.

This example shows how to configure an interface to receive NTP broadcast packets:

```
AP(config)# interface gigabitethernet0/1
AP(config-if)# ntp broadcast client
```

Configuring NTP Access Restrictions

You can control NTP access on two levels as described in these sections:

- Creating an Access Group and Assigning a Basic IP Access List, page 5-30
- Disabling NTP Services on a Specific Interface, page 5-31

Creating an Access Group and Assigning a Basic IP Access List

Beginning in privileged EXEC mode, follow these steps to control access to NTP services by using access lists:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*	Create an access group, and apply a basic IP access list. The keywords have these meanings: • **query-only**—Allows only NTP control queries. • **serve-only**—Allows only time requests. • **serve**—Allows time requests and NTP control queries, but does not allow the access point to synchronize to the remote device. • **peer**—Allows time requests and NTP control queries and allows the access point to synchronize to the remote device. For *access-list-number*, enter a standard IP access list number from 1 to 99.
Step 3	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	Create the access list. • For *access-list-number*, enter the number specified in Step 2. • Enter the **permit** keyword to permit access if the conditions are matched. • For *source*, enter the IP address of the device that is permitted access to the access point. • (Optional) For *source-wildcard*, enter the wildcard bits to be applied to the source. **Note** When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The access group keywords are scanned in this order, from least restrictive to most restrictive:

1. **peer**—Allows time requests and NTP control queries and allows the access point to synchronize itself to a device whose address passes the access list criteria.
2. **serve**—Allows time requests and NTP control queries, but does not allow the access point to synchronize itself to a device whose address passes the access list criteria.
3. **serve-only**—Allows only time requests from a device whose address passes the access list criteria.
4. **query-only**—Allows only NTP control queries from a device whose address passes the access list criteria.

If the source IP address matches the access lists for more than one access type, the first type is granted. If no access groups are specified, all access types are granted to all devices. If any access groups are specified, only the specified access types are granted.

To remove access control to the access point NTP services, use the **no ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} global configuration command.

This example shows how to configure the access point to allow itself to synchronize to a peer from access list 99. However, the access point restricts access to allow only time requests from access list 42:

```
AP# configure terminal
AP(config)# ntp access-group peer 99
AP(config)# ntp access-group serve-only 42
AP(config)# access-list 99 permit 172.20.130.5
AP(config)# access list 42 permit 172.20.130.6
```

Disabling NTP Services on a Specific Interface

NTP services are enabled on all interfaces by default.

Beginning in privileged EXEC mode, follow these steps to disable NTP packets from being received on an interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and specify the interface to disable.
Step 3	**ntp disable**	Disable NTP packets from being received on the interface. By default, all interfaces receive NTP packets.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To re-enable receipt of NTP packets on an interface, use the **no ntp disable** interface configuration command.

Configuring the Source IP Address for NTP Packets

When the access point sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use the **ntp source** global configuration command when you want to use a particular source IP address for all NTP packets. The address is taken from the specified interface. This command is useful if the address on an interface cannot be used as the destination for reply packets.

Beginning in privileged EXEC mode, follow these steps to configure a specific interface from which the IP source address is to be taken:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ntp source** *type number*	Specify the interface type and number from which the IP source address is taken. By default, the source address is determined by the outgoing interface.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The specified interface is used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** keyword in the **ntp peer** or **ntp server** global configuration command as described in the "Configuring NTP Associations" section on page 5-27.

Displaying the NTP Configuration

You can use two privileged EXEC commands to display NTP information:

- **show ntp associations** [**detail**]
- **show ntp status**

For detailed information about the fields in these displays, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.1*.

Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. Cisco recommends that you use manual configuration only as a last resort. If you have an outside source to which the access point can synchronize, you do not need to manually set the system clock.

This section contains this configuration information:

- Setting the System Clock, page 5-33
- Displaying the Time and Date Configuration, page 5-33
- Configuring the Time Zone, page 5-34
- Configuring Summer Time (Daylight Saving Time), page 5-35

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Beginning in privileged EXEC mode, follow these steps to set the system clock:

	Command	Purpose
Step 1	**clock set** *hh*:*mm*:*ss day month year* or **clock set** *hh*:*mm*:*ss month day year*	Manually set the system clock using one of these formats: • For *hh*:*mm*:*ss*, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. • For *day*, specify the day by date in the month. • For *month*, specify the month by name. • For *year*, specify the year (no abbreviation).
Step 2	**show running-config**	Verify your entries.
Step 3	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2001:

```
AP# clock set 13:32:00 23 July 2001
```

Displaying the Time and Date Configuration

To display the time and date configuration, use the **show clock** [**detail**] privileged EXEC command.

The system clock keeps an *authoritative* flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the *authoritative* flag is set, the flag prevents peers from synchronizing to the clock when the peers' time is invalid.

The symbol that precedes the **show clock** display has this meaning:

- *—Time is not authoritative.
- (blank)—Time is authoritative.
- .—Time is authoritative, but NTP is not synchronized.

Configuring the Time Zone

Beginning in privileged EXEC mode, follow these steps to manually configure the time zone:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	Set the time zone. The access point keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set. • For *zone*, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC. • For *hours-offset*, enter the hours offset from UTC. • (Optional) For *minutes-offset*, enter the minutes offset from UTC.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The *minutes-offset* variable in the **clock timezone** global configuration command is available for those cases where a local time zone is a percentage of an hour different from UTC. For example, the time zone for some sections of Atlantic Canada (AST) is UTC-3.5, where the 3 means 3 hours and .5 means 50 percent. In this case, the necessary command is **clock timezone AST -3 30**.

To set the time to UTC, use the **no clock timezone** global configuration command.

Configuring Summer Time (Daylight Saving Time)

Beginning in privileged EXEC mode, follow these steps to configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	Configure summer time to start and end on the specified days every year. Summer time is disabled by default. If you specify **clock summer-time** *zone* **recurring** without parameters, the summer time rules default to the United States rules. • For *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) For *week*, specify the week of the month (1 to 5 or **last**). • (Optional) For *day*, specify the day of the week (Sunday, Monday...). • (Optional) For *month*, specify the month (January, February...). • (Optional) For *hh*:*mm*, specify the time (24-hour format) in hours and minutes. • (Optional) For *offset*, specify the number of minutes to add during summer time. The default is 60.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

This example shows how to specify that summer time starts on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00:

```
AP(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

Beginning in privileged EXEC mode, follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] or **clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	Configure summer time to start on the first date and end on the second date. Summer time is disabled by default. • For *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) For *week*, specify the week of the month (1 to 5 or **last**). • (Optional) For *day*, specify the day of the week (Sunday, Monday...). • (Optional) For *month*, specify the month (January, February...). • (Optional) For *hh*:*mm*, specify the time (24-hour format) in hours and minutes. • (Optional) For *offset*, specify the number of minutes to add during summer time. The default is 60.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

To disable summer time, use the **no clock summer-time** global configuration command.

This example shows how to set summer time to start on October 12, 2000, at 02:00, and end on April 26, 2001, at 02:00:

```
AP(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

Configuring a System Name and Prompt

You configure the system name on the access point to identify it. By default, the system name and prompt are *ap*.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol (>) is appended. The prompt is updated whenever the system name changes, unless you manually configure the prompt by using the **prompt** global configuration command.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference* and the *Cisco IOS IP and IP Routing Command Reference for Release 12.1*.

This section contains this configuration information:

- Default System Name and Prompt Configuration, page 5-37
- Configuring a System Name, page 5-37
- Understanding DNS, page 5-38

Default System Name and Prompt Configuration

The default access point system name and prompt is *ap*.

Configuring a System Name

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**hostname** *name*	Manually configure a system name. The default setting is *ap*. **Note** When you change the system name, the access point radios reset, and associated client devices disassociate and quickly reassociate. **Note** You can enter up to 63 characters for the system name. However, when the access point identifies itself to client devices, it uses only the first 15 characters in the system name. If it is important for client users to distinguish between access points, make sure a unique portion of the system name appears in the first 15 characters.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

When you set the system name, it is also used as the system prompt.

To return to the default host name, use the **no hostname** global configuration command.

Understanding DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map host names to IP addresses. When you configure DNS on your access point, you can substitute the host name for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, such as the File Transfer Protocol (FTP) system, is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names, specify the name server that is present on your network, and enable the DNS.

This section contains this configuration information:

- Default DNS Configuration, page 5-38
- Setting Up DNS, page 5-39
- Displaying the DNS Configuration, page 5-40

Default DNS Configuration

Table 5-5 shows the default DNS configuration.

Table 5-5 Default DNS Configuration

Feature	Default Setting
DNS enable state	Disabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

Setting Up DNS

Beginning in privileged EXEC mode, follow these steps to set up your access point to use the DNS:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip domain-name** *name*	Define a default domain name that the software uses to complete unqualified host names (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the access point configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).
Step 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	Specify the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The access point sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	**ip domain-lookup**	(Optional) Enable DNS-based host name-to-address translation on your access point. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

If you use the access point IP address as its host name, the IP address is used and no DNS query occurs. If you configure a host name that contains no periods (.), a period followed by the default domain name is appended to the host name before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** global configuration command. If there is a period (.) in the host name, Cisco IOS software looks up the IP address without appending any default domain name to the host name.

To remove a domain name, use the **no ip domain-name** *name* global configuration command. To remove a name server address, use the **no ip name-server** *server-address* global configuration command. To disable DNS on the access point, use the **no ip domain-lookup** global configuration command.

Displaying the DNS Configuration

To display the DNS configuration information, use the **show running-config** privileged EXEC command.

Note When DNS is configured on the access point, the **show running-config** command sometimes displays a server's IP address instead of its name.

Creating a Banner

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner appears on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner also appears on all connected terminals. It appears after the MOTD banner and before the login prompts.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This section contains this configuration information:

- Default Banner Configuration, page 5-40
- Configuring a Message-of-the-Day Login Banner, page 5-40
- Configuring a Login Banner, page 5-42

Default Banner Configuration

The MOTD and login banners are not configured.

Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs into the access point.

Beginning in privileged EXEC mode, follow these steps to configure a MOTD login banner:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**banner motd** *c message c*	Specify the message of the day. For *c*, enter the delimiting character of your choice, such as a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For *message*, enter a banner message up to 255 characters. You cannot use the delimiting character in the message.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete the MOTD banner, use the **no banner motd** global configuration command.

This example shows how to configure a MOTD banner for the access point using the pound sign (#) symbol as the beginning and ending delimiter:

```
AP(config)# banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
AP(config)#
```

This example shows the banner displayed from the previous configuration:

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

User Access Verification

Password:
```

Configuring a Login Banner

You can configure a login banner to appear on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

Beginning in privileged EXEC mode, follow these steps to configure a login banner:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**banner login** *c message c*	Specify the login message. For *c*, enter the delimiting character of your choice, such as a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For *message*, enter a login message up to 255 characters. You cannot use the delimiting character in the message.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete the login banner, use the **no banner login** global configuration command.

This example shows how to configure a login banner for the access point using the dollar sign ($) symbol as the beginning and ending delimiter:

```
AP(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
AP(config)#
```

Configuring Radio Settings

This chapter describes how to configure radio settings for your access point. This chapter includes these sections:

- Disabling and Enabling the Radio Interface, page 6-2
- Configuring the Role in Radio Network, page 6-3
- Configuring Radio Data Rates, page 6-4
- Configuring Radio Transmit Power, page 6-6
- Configuring Radio Channel Settings, page 6-8
- Enabling and Disabling World-Mode, page 6-10
- Disabling and Enabling Short Radio Preambles, page 6-11
- Configuring Transmit and Receive Antennas, page 6-11
- Disabling and Enabling Aironet Extensions, page 6-12
- Configuring the Ethernet Encapsulation Transformation Method, page 6-13
- Enabling and Disabling Reliable Multicast to Workgroup Bridges, page 6-14
- Enabling and Disabling Public Secure Packet Forwarding, page 6-15
- Configuring the Beacon Period and the DTIM, page 6-16
- Configure RTS Threshold and Retries, page 6-16
- Configuring the Maximum Data Retries, page 6-17
- Configuring the Fragmentation Threshold, page 6-17
- Enabling Short Slot Time for 802.11g Radios, page 6-18
- Performing a Carrier Busy Test, page 6-18

Disabling and Enabling the Radio Interface

The access point radios are enabled by default. Beginning in privileged EXEC mode, follow these steps to disable the access point radio:

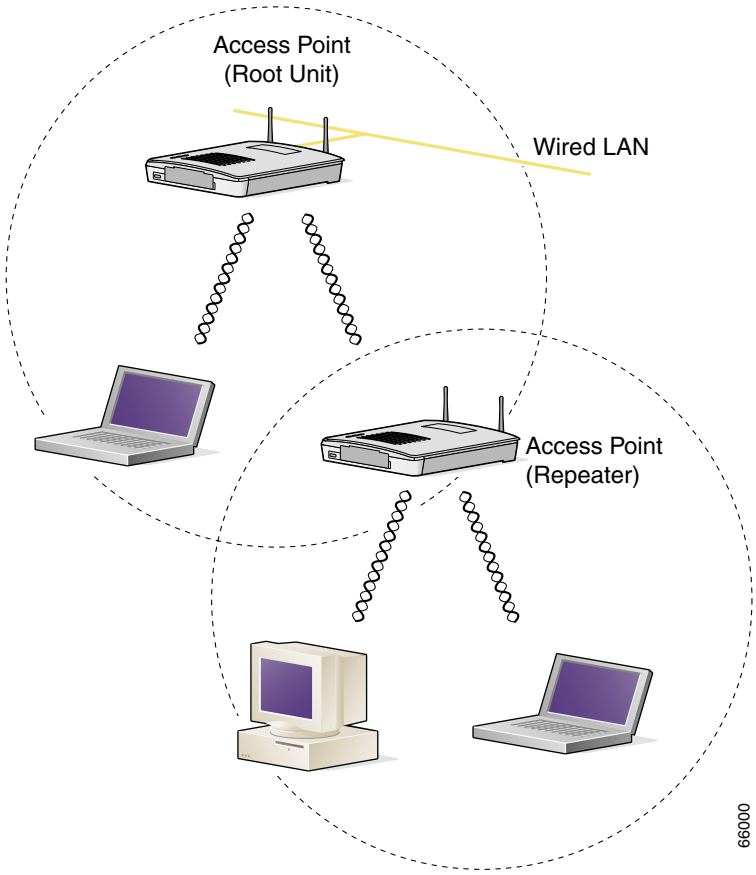
	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**shutdown**	Disable the radio port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the shutdown command to enable the radio port.

Configuring the Role in Radio Network

You can configure your access point as a root device that is connected to the wired LAN or as a repeater (non-root) device that is not connected to the wired LAN. Figure 6-1 shows root, scanner, and repeater access points.

Figure 6-1 Root and Repeater Access Points



See Chapter 19, "Configuring Repeater and Standby Access Points," for detailed instructions on setting up repeaters.

You can also configure a fallback role for root access points. The access point automatically assumes the fallback role when its Ethernet port is disabled or disconnected from the wired LAN. There are two possible fallback roles:

- Repeater—When the Ethernet port is disabled, the access point becomes a repeater and associates to a nearby root access point. You do not have to specify a root access point to which the fallback repeater associates; the repeater automatically associates to the root access point that provides the best radio connectivity.
- Shutdown—The access point shuts down its radio and disassociates all client devices.

Beginning in privileged EXEC mode, follow these steps to set the access point's radio network role and fallback role:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**station role repeater** | **root** [**fallback** { **shutdown** | **repeater** }]	Set the access point role. • Set the role to repeater or root. • (Optional) Select the root access point's fallback role. If the access point's Ethernet port is disabled or disconnected from the wired LAN, the access point can either shut down its radio port or become a repeater access point associated to any nearby root access point.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring Radio Data Rates

You use the data rate settings to choose the data rates the access point uses for data transmission. The rates are expressed in megabits per second. The access point always attempts to transmit at the highest data rate set to **Basic**, also called **Require** on the browser-based interface. If there are obstacles or interference, the access point steps down to the highest rate that allows data transmission. You can set each data rate to one of three states:

- Basic (the GUI labels Basic rates as Required)—Allows transmission at this rate for all packets, both unicast and multicast. At least one of the access point's data rates must be set to Basic.
- Enabled—The access point transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.
- Disabled—The access point does not transmit data at this rate.

Note At least one data rate must be set to **basic**.

You can use the Data Rate settings to set up an access point to serve client devices operating at specific data rates. For example, to set up the 2.4-GHz radio for 11 megabits per second (Mbps) service only, set the 11-Mbps rate to **Basic** and set the other data rates to **Disabled**. To set up the access point to serve only client devices operating at 1 and 2 Mbps, set 1 and 2 to **Basic** and set the rest of the data rates to **Disabled**. To set up the 2.4-GHz, 802.11g radio to serve only 802.11g client devices, set any Orthogonal Frequency Division Multiplexing (OFDM) data rate (6, 9, 12, 18, 24, 36, 48, 54) to **Basic**. To set up the 5-GHz radio for 54 Mbps service only, set the 54-Mbps rate to **Basic** and set the other data rates to **Disabled**.

You can also configure the access point to set the data rates automatically to optimize either range or throughput. When you enter **range** for the data rate setting, the access point sets the 1 Mbps rate to basic and the other rates to **enabled**. When you enter throughput for the data rate setting, the access point sets all four data rates to **basic**.

Beginning in privileged EXEC mode, follow these steps to configure the radio data rates:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**speed** These options are available for the 802.11b, 2.4-GHz radio: {[**1.0**] [**11.0**] [**2.0**] [**5.5**] [**basic-1.0**] [**basic-11.0**] [**basic-2.0**] [**basic-5.5**] | **range** | **throughput**} These options are available for the 802.11g, 2.4-GHz radio: {[**1.0**] [**2.0**] [**5.5**] [**6.0**] [**9.0**] [**11.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-1.0**] [**basic-2.0**] [**basic-5.5**] [**basic-6.0**] [**basic-9.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** | **default** } These options are available for the 5-GHz radio: {[**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-6.0**] [**basic-9.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** | **default** }	Set each data rate to **basic** or **enabled**, or enter **range** to optimize access point range or **throughput** to optimize throughput. • (Optional) Enter **1.0**, **2.0**, **5.5**, and **11.0** to set these data rates to **enabled** on the 802.11b, 2.4-GHz radio. Enter **1.0**, **2.0**, **5.5**, **6.0**, **9.0**, **11.0**, **12.0**, **18.0**, **24.0**, **36.0**, **48.0**, and **54.0** to set these data rates to **enabled** on the 802.11g, 2.4-GHz radio. Enter **6.0**, **9.0**, **12.0**, **18.0**, **24.0**, **36.0**, **48.0**, and **54.0** to set these data rates to **enabled** on the 5-GHz radio. • (Optional) Enter **basic-1.0**, **basic-2.0**, **basic-5.5**, and **basic-11.0** to set these data rates to **basic** on the 802.11b, 2.4-GHz radio. Enter **basic-1.0**, **basic-2.0**, **basic-5.5**, **basic-6.0**, **basic-9.0**, **basic-11.0**, **basic-12.0**, **basic-18.0**, **basic-24.0**, **basic-36.0**, **basic-48.0**, and **basic-54.0** to set these data rates to **basic** on the 802.11g, 2.4-GHz radio. **Note** The client must support the basic rate that you select or it cannot associate to the access point. If you select 12 Mbps or higher for the basic data rate on the 802.11g radio, 802.11b client devices cannot associate to the access point's 802.11g radio. Enter **basic-6.0**, **basic-9.0**, **basic-12.0**, **basic-18.0**, **basic-24.0**, **basic-36.0**, **basic-48.0**, and **basic-54.0** to set these data rates to **basic** on the 5-GHz radio. • (Optional) Enter **range** or **throughput** to automatically optimize radio range or throughput. When you enter **range**, The access point sets the lowest data rate to basic and the other rates to **enabled**. When you enter **throughput**, the access point sets all data rates to **basic**. • (Optional) Enter **default** to set the data rates to factory default settings. This option is not supported on the 2.4-GHz, 802.11b radio. On the 802.11g radio, the **default** option sets data rates 1, 2, 5.5, and 11 to basic, and data rates 6, 9, 12, 18, 24, 36, 48, and 54 to enabled. These data rate settings allow both 802.11b and 802.11g client devices to associate to the access point's 802.11g radio. On the 5-GHz radio, the **default** option sets data rates 6.0, 12.0, and 24.0 to basic, and data rates 9.0, 18.0, 36.0, 48.0, and 54.0 to enabled.

	Command	Purpose
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the **speed** command to disable data rates. When you use the **no** form of the command, all data rates are disabled except the rates you name in the command. This example shows how to disable data rate 1.0:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no speed basic-2.0 basic-5.5 basic-11.0
ap1200(config-if)# end
```

Data rate 1 is disabled, and the rest of the rates are set to basic.

This example shows how to set up the access point for 11-Mbps service only:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no speed basic-11.0
ap1200(config-if)# end
```

Data rate 11 is set to basic, and the rest of the data rates are set to disabled.

Configuring Radio Transmit Power

Beginning in privileged EXEC mode, follow these steps to set the transmit power on access point radios:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**power local** These options are available for the 802.11b, 2.4-GHz radio: { **1** | **5** | **20** | **30** | **50** | **100** | **maximum** } These options are available for the 5-GHz radio: { **5** | **10** | **20** | **40** | **maximum** }	Set the transmit power for the 802.11b, 2.4-GHz radio or the 5-GHz radio to one of the power levels allowed in your regulatory domain. All settings are in mW. **Note** The settings allowed in your regulatory domain might differ from the settings listed here.

	Command	Purpose
Step 4	**power local** These options are available for the 802.11g, 2.4-GHz radio: **power local cck** settings: { **1** | **5** | **10** | **20** | **30** | **50** | **100** | **maximum** } **power local ofdm** settings: { **1** | **5** | **10** | **20** | **30** | **maximum** }	Set the transmit power for the 802.11g, 2.4-GHz radio to one of the power levels allowed in your regulatory domain. All settings are in mW. On the 2.4-GHz, 802.11g radio, you can set Orthogonal Frequency Division Multiplexing (OFDM) power levels and Complementary Code Keying (CCK) power levels. CCK modulation is supported by 802.11b and 802.11g devices. OFDM modulation is supported by 802.11g and 802.11a devices. **Note** The settings allowed in your regulatory domain might differ from the settings listed here. **Note** The 802.11g radio transmits at up to 100 mW for the 1, 2, 5.5, and 11Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the power command to return the power setting to **maximum**, the default setting.

Limiting the Power Level for Associated Client Devices

You can also limit the power level on client devices that associate to the access point. When a client device associates to the access point, the access point sends the maximum power level setting to the client.

Beginning in privileged EXEC mode, follow these steps to specify a maximum allowed power setting on all client devices that associate to the access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	**power client** These options are available for 802.11b, 2.4-GHz clients: { **1** | **5** | **20** | **30** | **50** | **100** | **maximum**} These options are available for 802.11g, 2.4-GHz clients: { **1** | **5** | **10** | **20** | **30** | **50** | **100** | **maximum**} These options are available for 5-GHz clients: { **5** | **10** | **20** | **40** | **maximum** }	Set the maximum power level allowed on client devices that associate to the access point. All settings are in mW. **Note** The settings allowed in your regulatory domain might differ from the settings listed here.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the client power command to disable the maximum power level for associated clients.

Note Aironet extensions must be enabled to limit the power level on associated client devices. Aironet extensions are enabled by default.

Configuring Radio Channel Settings

The default channel setting for the access point radios is least congested; at startup, the access point scans for and selects the least-congested channel. For most consistent performance after a site survey, however, we recomend that you assign a static channel setting for each access point. The channel settings on your access point correspond to the frequencies available in your regulatory domain. See Appendix A, "Channels and Antenna Settings," for the frequencies allowed in your domain.

Each 2.4-GHz channel covers 22 MHz. The bandwidth for channels 1, 6, and 11 does not overlap, so you can set up multiple access points in the same vicinity without causing interference. Both 802.11b and 802.11g 2.4-GHz radios use the same channels and frequencies.

The 5-GHz radio operates on eight channels from 5180 to 5320 MHz. Each channel covers 20 MHz, and the bandwidth for the channels overlaps slightly. For best performance, use channels that are not adjacent (44 and 46, for example) for radios that are close to each other.

Note Too many access points in the same vicinity creates radio congestion that can reduce throughput. A careful site survey can determine the best placement of access points for maximum radio coverage and throughput.

Beginning in privileged EXEC mode, follow these steps to set the access point's radio channel:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**channel** *frequency* | **least-congested**	Set the default channel for the access point radio. To search for the least-congested channel on startup, enter **least-congested**. These are the available frequencies (in MHz) for the 2.4-GHz radio: • channel 1—**2412** (Americas, EMEA, Japan, and China) • channel 2—**2417** (Americas, EMEA, Japan, and China) • channel 3—**2422** (Americas, EMEA, Japan, Israel, and China) • channel 4—**2427** (Americas, EMEA, Japan, Israel, and China) • channel 5—**2432** (Americas, EMEA, Japan, Israel, and China) • channel 6—**2437** (Americas, EMEA, Japan, Israel, and China) • channel 7—**2442** (Americas, EMEA, Japan, Israel, and China) • channel 8—**2447** (Americas, EMEA, Japan, Israel, and China) • channel 9—**2452** (Americas, EMEA, Japan, Israel, and China) • channel 10—**2457** (Americas, EMEA, Japan, and China) • channel 11—**2462** (Americas, EMEA, Japan, and China) • channel 12—**2467** (EMEA and Japan only) • channel 13—**2472** (EMEA and Japan only) • channel 14—**2484** (Japan only) These are the available frequencies (in MHz) for the 5-GHz radio: • channel 34—**5170** (Japan only) • channel 36—**5180** (Americas and Singapore) • channel 38—**5190** (Japan only) • channel 40—**5200** (Americas and Singapore) • channel 42—**5210** (Japan only) • channel 44—**5220** (Americas and Singapore) • channel 46—**5230** (Japan only) • channel 48—**5240** (Americas and Singapore) • channel 52—**5260** (Americas and Taiwan) • channel 56—**5280** (Americas and Taiwan) • channel 60—**5300** (Americas and Taiwan) • channel 64—**5320** (Americas and Taiwan) **Note** The frequencies allowed in your regulatory domain might differ from the frequencies listed here.

	Command	Purpose
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Enabling and Disabling World-Mode

You can configure the access point to support 802.11d world mode or Cisco legacy world mode. When you enable world mode, the access point adds channel carrier set information to its beacon. Client devices with world mode enabled receive the carrier set information and adjust their settings automatically. For example, a client device used primarily in Japan could rely on world mode to adjust its channel and power settings automatically when it travels to Italy and joins a network there. Cisco client devices running firmware version 5.30.17 or later detect whether the access point is using 802.11d or Cisco legacy world mode and automatically use world mode that matches the mode used by the access point. World mode is disabled by default.

World mode is not supported on the 5-GHz radio.

Beginning in privileged EXEC mode, follow these steps to enable world mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio 0**	Enter interface configuration mode for the 2.4-GHz radio interface.
Step 3	**world-mode dot11d country_code** *code* { **both** | **indoor** | **outdoor** } | **legacy**	Enable world mode. • Enter the **dot11d** option to enable 802.11d world mode. – When you enter the **dot11d** option, you must enter a two-character ISO country code (for example, the ISO country code for the United States is **US**). You can find a list of ISO country codes at the ISO website. – After the country code, you must enter **indoor**, **outdoor**, or **both** to indicate the placement of the access point. • Enter the **legacy** option to enable Cisco legacy world mode. **Note** Aironet extensions must be enabled for legacy world mode operation, but Aironet extensions are not required for 802.11d world mode. Aironet extensions are enabled by default.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable world mode.

Disabling and Enabling Short Radio Preambles

The radio preamble (sometimes called a *header*) is a section of data at the head of a packet that contains information that the access point and client devices need when sending and receiving packets. You can set the radio preamble to long or short:

- Short—A short preamble improves throughput performance. Cisco Aironet Wireless LAN Client Adapters support short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.
- Long—A long preamble ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). If these client devices do not associate to your access points, you should use short preambles.

You cannot configure short or long radio preambles on the 5-GHz radio.

Beginning in privileged EXEC mode, follow these steps to disable short radio preambles:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio 0**	Enter interface configuration mode for the 2.4-GHz radio interface.
Step 3	**no preamble-short**	Disable short preambles and enable long preambles.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Short preambles are enabled by default. Use the **preamble-short** command to enable short preambles if they are disabled.

Configuring Transmit and Receive Antennas

You can select the antenna the access point uses to receive and transmit data. There are three options for both the receive and the transmit antenna:

- Diversity—This default setting tells the access point to use the antenna that receives the best signal. If your access point has two fixed (non-removeable) antennas, you should use this setting for both receive and transmit.
- Right—If your access point has removeable antennas and you install a high-gain antenna on the access point's right connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the right antenna is on the right.
- Left—If your access point has removeable antennas and you install a high-gain antenna on the access point's left connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the left antenna is on the left.

Beginning in privileged EXEC mode, follow these steps to select the antennas the access point uses to receive and transmit data:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**antenna receive** {**diversity** | **left** | **right**}	Set the receive antenna to diversity, left, or right. **Note** For best performance, leave the receive antenna setting at the default setting, **diversity**.
Step 4	**antenna transmit** {**diversity** | **left** | **right**}	Set the transmit antenna to diversity, left, or right. **Note** For best performance, leave the transmit antenna setting at the default setting, **diversity**.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Disabling and Enabling Aironet Extensions

By default, the access point uses Cisco Aironet 802.11 extensions to detect the capabilities of Cisco Aironet client devices and to support features that require specific interaction between the access point and associated client devices. Aironet extensions must be enabled to support these features:

- Load balancing—The access point uses Aironet extensions to direct client devices to an access point that provides the best connection to the network based on factors such as number of users, bit error rates, and signal strength.
- Message Integrity Check (MIC)—MIC is an additional WEP security feature that prevents attacks on encrypted packets called bit-flip attacks. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.
- Cisco Key Integrity Protocol (CKIP)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group. The standards-based algorithm, TKIP, does not require Aironet extensions to be enabled.
- Repeater mode—Aironet extensions must be enabled on repeater access points and on the root access points to which they associate.
- World mode (legacy only)—Client devices with legacy world mode enabled receive carrier set information from the access point and adjust their settings automatically. Aironet extensions are not required for 802.11d world mode operation.
- Limiting the power level on associated client devices—When a client device associates to the access point, the access point sends the maximum allowed power level setting to the client.

Disabling Aironet extensions disables the features listed above, but it sometimes improves the ability of non-Cisco client devices to associate to the access point.

Aironet extensions are enabled by default. Beginning in privileged EXEC mode, follow these steps to disable Aironet extensions:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**no dot11 extension aironet**	Disable Aironet extensions.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **dot11 extension aironet** command to enable Aironet extensions if they are disabled.

Configuring the Ethernet Encapsulation Transformation Method

When the access point receives data packets that are not 802.3 packets, the access point must format the packets to 802.3 using an encapsulation transformation method. These are the two transformation methods:

- 802.1H—This method provides optimum performance for Cisco Aironet wireless products. This is the default setting.
- RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. RFC1042 does not provide the interoperability advantages of 802.1H but is used by other manufacturers of wireless equipment.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**payload-encapsulation** **snap** | **dot1h**	Set the encapsulation transformation method to RFC1042 (**snap**) or 802.1h (**dot1h**, the default setting).
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Enabling and Disabling Reliable Multicast to Workgroup Bridges

The *Reliable multicast messages from the access point to workgroup bridges* setting limits reliable delivery of multicast messages to approximately 20 Cisco Aironet Workgroup Bridges that are associated to the access point. The default setting, **disabled**, reduces the reliability of multicast delivery to allow more workgroup bridges to associate to the access point.

Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

The performance cost of reliable multicast delivery—duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to the access point. To increase beyond 20 the number of workgroup bridges that can maintain a radio link to the access point, the access point must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the access point cannot confirm whether multicast packets reach the intended workgroup bridge, so workgroup bridges at the edge of the access point's coverage area might lose IP connectivity. When you treat workgroup bridges as client devices, you increase performance but reduce reliability.

Note This feature is best suited for use with stationary workgroup bridges. Mobile workgroup bridges might encounter spots in the access point's coverage area where they do not receive multicast packets and lose communication with the access point even though they are still associated to it.

A Cisco Aironet Workgroup Bridge provides a wireless LAN connection for up to eight Ethernet-enabled devices.

This feature is not supported on the 5-GHz radio.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio 0**	Enter interface configuration mode for the 2.4-GHz radio interface.
Step 3	**infrastructure-client**	Enable reliable multicast messages to workgroup bridges.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable reliable multicast messages to workgroup bridges.

Enabling and Disabling Public Secure Packet Forwarding

Public Secure Packet Forwarding (PSPF) prevents client devices associated to an access point from inadvertently sharing files or communicating with other client devices associated to the access point. It provides Internet access to client devices without providing other capabilities of a LAN. This feature is useful for public wireless networks like those installed in airports or on college campuses.

Note To prevent communication between clients associated to different access points, you must set up protected ports on the switch to which your access points are connected. See the "Configuring Protected Ports" section on page 6-15 for instructions on setting up protected ports.

To enable and disable PSPF using CLI commands on your access point, you use bridge groups. You can find a detailed explanation of bridge groups and instructions for implementing them in this document:

- *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*. Click this link to browse to the Configuring Transparent Bridging chapter: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart1/bcftb.htm

You can also enable and disable PSPF using the web-browser interface. The PSPF setting is on the Radio Settings pages.

PSPF is disabled by default. Beginning in privileged EXEC mode, follow these steps to enable PSPF:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**bridge-group** *group* **port-protected**	Enable PSPF.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable PSPF.

Configuring Protected Ports

To prevent communication between client devices associated to different access points on your wireless LAN, you must set up protected ports on the switch to which your access points are connected. Follow these steps to set up protected ports on your switch:

Beginning in privileged EXEC mode, follow these steps to define a port on your switch as a protected port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the type and number of the switchport interface to configure, such as **gigabitethernet0/1**.

	Command	Purpose
Step 3	**switchport protected**	Configure the interface to be a protected port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable protected port, use the **no switchport protected** interface configuration command.

For detailed information on protected ports and port blocking, refer to the "Configuring Port-Based Traffic Control" chapter in the *Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EA1*. Click this link to browse to that guide:

http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_book09186a008011591c.html

Configuring the Beacon Period and the DTIM

The beacon period is the amount of time between access point beacons in Kilomicroseconds. One Kμsec equals 1,024 microseconds. The Data Beacon Rate, always a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them.

For example, if the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 Kμsecs. One Kμsec equals 1,024 microseconds.

The default beacon period is 100, and the default DTIM is 2. Beginning in privileged EXEC mode, follow these steps to configure the beacon period and the DTIM:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**beacon period** *value*	Set the beacon period. Enter a value in Kilomicroseconds.
Step 4	**beacon dtim-period** *value*	Set the DTIM. Enter a value in Kilomicroseconds.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configure RTS Threshold and Retries

The RTS threshold determines the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other. You can enter a setting ranging from 0 to 2339 bytes.

Maximum RTS Retries is the maximum number of times the access point issues an RTS before stopping the attempt to send the packet over the radio. Enter a value from 1 to 128.

The default RTS threshold is 2312, and the default maximum RTS retries setting is 32. Beginning in privileged EXEC mode, follow these steps to configure the RTS threshold and maximum RTS retries:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**rts threshold** *value*	Set the RTS threshold. Enter an RTS threshold from 0 to 2339.
Step 4	**rts retries** *value*	Set the maximum RTS retries. Enter a setting from 1 to 128.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the RTS settings to defaults.

Configuring the Maximum Data Retries

The maximum data retries setting determines the number of attempts the access point makes to send a packet before giving up and dropping the packet.

The default setting is 32. Beginning in privileged EXEC mode, follow these steps to configure the maximum data retries:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**packet retries** *value*	Set the maximum data retries. Enter a setting from 1 to 128.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

Configuring the Fragmentation Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

The default setting is 2338 bytes. Beginning in privileged EXEC mode, follow these steps to configure the fragmentation threshold:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**fragment-threshold** *value*	Set the fragmentation threshold. Enter a setting from 256 to 2346 bytes for the 2.4-GHz radio. Enter a setting from 256 to 2346 bytes for the 5-GHz radio.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

Enabling Short Slot Time for 802.11g Radios

You can increase throughput on the 802.11g, 2.4-GHz radio by enabling short slot time. Reducing the slot time from the standard 20 microseconds to the 9-microsecond short slot time decreases the overall backoff, which increases throughput. Backoff, which is a multiple of the slot time, is the random length of time that a station waits before sending a packet on the LAN.

Many 802.11g radios support short slot time, but some do not. When you enable short slot time, the access point uses the short slot time only when all clients associated to the 802.11g, 2.4-GHz radio support short slot time.

Short slot time is supported only on the 802.11g, 2.4-GHz radio. Short slot time is disabled by default.

In radio interface mode, enter this command to enable short slot time:

ap(config-if)# **slot-time-short**

Enter **no slot-time-short** to disable short slot time.

Performing a Carrier Busy Test

You can perform a carrier busy test to check the radio activity on access point channels. During the carrier busy test, the access point drops all associations with wireless networking devices for around 4 seconds while it conducts the carrier test and then displays the test results.

In privileged EXEC mode, enter this command to perform a carrier busy test:

dot11 *interface-number* **carrier busy**

For *interface-number*, enter **dot11radio 0** to run the test on the 2.4-GHz radio, or enter **dot11radio 1** to run the test on the 5-GHz radio.

Use the **show dot11 carrier busy** command to re-display the carrier busy test results.

Configuring Multiple SSIDs

This chapter describes how to configure and manage multiple service set identifiers (SSIDs) on the access point. This chapter contains these sections:

- Understanding Multiple SSIDs, page 7-2
- Configuring Multiple SSIDs, page 7-2

Understanding Multiple SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSIDs.

You can configure up to 16 SSIDs on your 1200 series access point and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point using any of the SSIDs. These are the settings you can assign to each SSID:

- VLAN
- Client authentication method

Note For detailed information on client authentication types, see Chapter 10, "Configuring Authentication Types."

- Maximum number of client associations using the SSID
- Proxy mobile IP
- RADIUS accounting for traffic using the SSID
- Guest mode
- Repeater mode, including authentication username and password

If you want the access point to allow associations from client devices that do not specify an SSID in their configurations, you can set up a guest SSID. The access point includes the guest SSID in its beacon. The access point's default SSID, *tsunami*, is set to guest mode. However, to keep your network secure, you should disable the guest mode SSID on most access points.

If your access point will be a repeater or will be a root access point that acts as a parent for a repeater, you can set up an SSID for use in repeater mode. You can assign an authentication username and password to the repeater-mode SSID to allow the repeater to authenticate to your network like a client device.

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.

Configuring Multiple SSIDs

These sections contain configuration information for multiple SSIDs:

- Default SSID Configuration, page 7-3
- Creating an SSID, page 7-3
- Using a RADIUS Server to Restrict SSIDs, page 7-5

Default SSID Configuration

Table 7-1 shows the default SSID configuration:

Table 7-1 Default SSID Configuration

Feature	Default Setting
SSID	tsunami
Guest Mode SSID	tsunami (The access point broadcasts this SSID in its beacon and allows client devices with no SSID to associate.)

Creating an SSID

Beginning in privileged EXEC mode, follow these steps to create an SSID:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.
Step 4	**authentication client username** *username* **password** *password*	(Optional) Set an authentication username and password that the access point uses to authenticate to the network when in repeater mode. Set the username and password on the SSID that the repeater access point uses to associate to a root access point, or with another repeater.
Step 5	**accounting** *list-name*	(Optional) Enable RADIUS accounting for this SSID. For *list-name*, specify the accounting method list. Click this link for more information on method lists: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2
Step 6	**vlan** *vlan-id*	(Optional) Assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. You can assign only one SSID to a VLAN.
Step 7	**guest-mode**	(Optional) Designate the SSID as your access point's guest-mode SSID. The access point includes the SSID in its beacon and allows associations from client devices that do not specify an SSID.

	Command	Purpose
Step 8	**infrastructure-ssid** [**optional**]	(Optional) Designate the SSID as the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. If you designate an SSID as the infrastructure SSID, infrastructure devices must associate to the access point using that SSID unless you also enter the **optional** keyword.
Step 9	**end**	Return to privileged EXEC mode.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note You use the **ssid** command's authentication options to configure an authentication type for each SSID. See Chapter 10, "Configuring Authentication Types,"for instructions on configuring authentication types.

Use the **no** form of the command to disable the SSID or to disable SSID features.

This example shows how to:

- Name an SSID
- Configure the SSID for RADIUS accounting
- Set the maximum number of client devices that can associate using this SSID to 15
- Assign the SSID to a VLAN

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# end
```

Using Spaces in SSIDs

You can include spaces in an SSID, but be careful not to add spaces to an SSID accidentally, especially trailing spaces (spaces at the end of an SSID). If you add trailing spaces, it might appear that you have identical SSIDs configured on the same access point. If you think you configured identical SSIDs on the access point, use the **show dot11 associations** privileged EXEC command to check your SSIDs for trailing spaces.

For example, this sample output from a **show configuration** privileged EXEC command does not show spaces in SSIDs:

```
ssid buffalo
    vlan 77
    authentication open

ssid buffalo
    vlan 17
    authentication open
```

```
ssid buffalo
    vlan 7
    authentication open
```

However, this sample output from a **show dot11 associations** privileged EXEC command shows the spaces in the SSIDs:

```
SSID [buffalo] :

SSID [buffalo ] :

SSID [buffalo  ] :
```

Using a RADIUS Server to Restrict SSIDs

To prevent client devices from associating to the access point using an unauthorized SSID, you can create a list of authorized SSIDs that clients must use on your RADIUS authentication server.

The SSID authorization process consists of these steps:

1. A client device associates to the access point using any SSID configured on the access point.
2. The client begins RADIUS authentication.
3. The RADIUS server returns a list of SSIDs that the client is allowed to use. The access point checks the list for a match of the SSID used by the client. There are three possible outcomes:
   a. If the SSID that the client used to associate to the access point matches an entry in the allowed list returned by the RADIUS server, the client is allowed network access after completing all authentication requirements.
   b. If the access point does not find a match for the client in the allowed list of SSIDs, the access point disassociates the client.
   c. If the RADIUS server does not return any SSIDs (no list) for the client, then the administrator has not configured the list, and the client is allowed to associate and attempt to authenticate.

The allowed list of SSIDs from the RADIUS server are in the form of Cisco VSAs. The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the access point and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named *cisco-avpair*. The Radius server is allowed to have zero or more SSID VSAs per client.

In this example, the following AV pair adds the SSID *batman* to the list of allowed SSIDs for a user:

```
cisco-avpair= "ssid=batman"
```

For instructions on configuring the access point to recognize and use VSAs, see the "Configuring the Access Point to Use Vendor-Specific RADIUS Attributes" section on page 12-14.

CHAPTER 8

Configuring an Access Point as a Local Authenticator

This chapter describes how to configure the access point as a local authenticator to serve as a stand-alone authenticator for a small wireless LAN or to provide backup authentication service. As a local authenticator, the access point performs both LEAP and MAC-based authentication for up to 50 client devices. This chapter contains these sections:

- Understanding Local Authentication, page 8-2
- Configuring a Local Authenticator, page 8-2

Understanding Local Authentication

Many small wireless LANs that could be made more secure with 802.1x authentication do not have access to a RADIUS server. On many wireless LANs that use 802.1x authentication, access points rely on RADIUS servers housed in a distant location to authenticate client devices, and the authentication traffic must cross a WAN link. If the WAN link fails, or if the access points cannot access the RADIUS servers for any reason, client devices cannot access the wireless network even if the work they wish to do is entirely local.

To provide local authentication service or backup authentication service in case of a WAN link or a server failure, you can configure an access point to act as a local authentication server. The access point can authenticate up to 50 wireless client devices using LEAP or MAC-based authentication. The access point performs up to 5 authentications per second.

You configure the local authenticator access point manually with client usernames and passwords because it does not synchronize its database with the main RADIUS servers. You can also specify a VLAN and a list of SSIDs that a client is allowed to use.

Note If your wireless LAN contains only one access point, you can configure the access point as both the 802.1x authenticator and the local authenticator. However, users associated to the local authenticator access point might notice a drop in performance when the access point authenticates client devices.

You can configure your access points to use the local authenticator when they cannot reach the main servers, or you can configure your access points to use the local authenticator or as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your main servers, the access points periodically check the link to the main servers and stop using the local authenticator automatically when the link to the main servers is restored.

Caution The access point you use as an authenticator contains detailed authentication information for your wireless LAN, so you should secure it physically to protect its configuration.

Configuring a Local Authenticator

This section provides instructions for setting up an access point as a local authenticator and includes these sections:

- Guidelines for Local Authenticators, page 8-3
- Configuration Overview, page 8-3
- Configuring the Local Authenticator Access Point, page 8-3
- Configuring Other Access Points to Use the Local Authenticator, page 8-6
- Unblocking Locked Usernames, page 8-7
- Viewing Local Authenticator Statistics, page 8-7
- Using Debug Messages, page 8-7

Guidelines for Local Authenticators

Follow these guidelines when configuring an access point as a local authenticator:

- Use an access point that does not serve a large number of client devices. When the access point acts as an authenticator, performance might degrade for associated client devices.
- Secure the access point physically to protect its configuration.

Configuration Overview

You complete four major steps when you set up a local authenticator:

1. On the local authenticator, create a list of access points authorized to use the authenticator to authenticate client devices. Each access point that uses the local authenticator is a Network Access Server (NAS).

   Note If your local authenticator access point also serves client devices, you must enter the local authenticator access point as a NAS. When a client associates to the local authenticator access point, the access point uses itself to authenticate the client.

2. On the local authenticator, create user groups and configure parameters to be applied to each group (optional).
3. On the local authenticator, create a list of up to 50 LEAP users or MAC addresses that the local authenticator is authorized to authenticate.
4. On the access points that use the local authenticator, enter the local authenticator as a RADIUS server.

   Note If your local authenticator access point also serves client devices, you must enter the local authenticator as a RADIUS server in the local authenticator's configuration. When a client associates to the local authenticator access point, the access point uses itself to authenticate the client.

Configuring the Local Authenticator Access Point

Beginning in Privileged Exec mode, follow these steps to configure the access point as a local authenticator:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**radius-server local**	Enable the access point as a local authenticator and enter configuration mode for the authenticator.

	Command	Purpose
Step 4	**nas** *ip-address* **key** *shared-key*	Add an access point to the list of units that use the local authenticator. Enter the access point's IP address and the shared key used to authenticate communication between the local authenticator and other access points. You must enter this shared key on the access points that use the local authenticator. If your local authenticator also serves client devices, you must enter the local authenticator access point as a NAS. **Note** Leading spaces in the key string are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. Repeat this step to add each access point that uses the local authenticator.
Step 5	**group** *group-name*	(Optional) Enter user group configuration mode and configure a user group to which you can assign shared settings.
Step 6	**vlan** *vlan*	(Optional) Specify a VLAN to be used by members of the user group. The access point moves group members into that VLAN, overriding other VLAN assignments. You can assign only one VLAN to the group.
Step 7	**ssid** *ssid*	(Optional) Enter up to 20 SSIDs to limit members of the user group to those SSIDs. The access point checks that the SSID that the client used to associate matches one of the SSIDs in the list. If the SSID does not match, the client is disassociated.
Step 8	**reauthentication time** *seconds*	(Optional) Enter the number of seconds after which access points should reauthenticate members of the group. The reauthentication provides users with a new encryption key. The default setting is 0, which means that group members are never required to reauthenticate.
Step 9	**lockout count** *count* **time** { *seconds* | **infinite** }	(Optional) To help protect against password guessing attacks, you can lock out group members for a length of time after a set number of incorrect passwords. • count—The number of failed passwords that triggers a lockout of the user name. • time—The number of seconds the lockout should last. If you enter **infinite**, an administrator must manually unblock the locked user name. See the "Unblocking Locked Usernames" section on page 8-7 for instructions on unblocking client devices.
Step 10	**exit**	Exit group configuration mode and return to authenticator configuration mode.

	Command	Purpose
Step 11	**user** *username* { **password** | **nthash** } *password* [**group** *group-name*]	Enter the users allowed to authenticate using the local authenticator. You must enter a user name and password for each user. If you only know the NT value of the password, which you can often find in the authentication server database, you can enter the NT hash as a string of hexadecimal digits. To add a client device for MAC-based authentication, enter the client's MAC address as both the username and password. To add the user to a user group, enter the group name. If you do not specify a group, the user is not assigned to a specific VLAN and is never forced to reauthenticate.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to set up a local authenticator used by three access points with three user groups and several users:

```
AP# configure terminal
AP(config)# radius-server local
AP(config-radsrv)# nas 10.91.6.159 key 110337
AP(config-radsrv)# nas 10.91.6.162 key 110337
AP(config-radsrv)# nas 10.91.6.181 key 110337
AP(config-radsrv)# group clerks
AP(config-radsrv-group)# vlan 87
AP(config-radsrv-group)# ssid batman
AP(config-radsrv-group)# ssid robin
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# lockout count 2 time 600
AP(config-radsrv-group)# group cashiers
AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# lockout count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# lockout count 2 time 600
AP(config-radsrv-group)# exit
AP(config-radsrv)# user jsmith password twain74 group clerks
AP(config-radsrv)# user stpatrick password snake100 group clerks
AP(config-radsrv)# user nick password uptown group clerks
AP(config-radsrv)# user 00095125d02b password 00095125d02b group cashiers
AP(config-radsrv)# user 00079431f04a password 00079431f04a group cashiers
AP(config-radsrv)# user carl password 272165 group managers
AP(config-radsrv)# user vic password lid178 group managers
AP(config-radsrv)# end
```

Configuring Other Access Points to Use the Local Authenticator

You add the local authenticator to the list of servers on the access point the same way that you add other servers. For detailed instructions on setting up RADIUS servers on your access points, see Chapter 12, "Configuring RADIUS and TACACS+ Servers."

Note If your local authenticator access point also serves client devices, you must configure the local authenticator to use itself to authenticate client devices.

On the access points that use the local authenticator, use the **radius-server host** command to enter the local authenticator as a RADIUS server. The order in which the access point attempts to use the servers matches the order in which you enter the servers in the access point configuration. If you are configuring the access point to use RADIUS for the first time, enter the main RADIUS servers first, and enter the local authenticator last.

Note You must enter **1812** as the authentication port and **1813** as the accounting port. The local authenticator listens on UDP port 1813 for RADIUS accounting packets. It discards the accounting packets but sends acknowledge packets back to RADIUS clients to prevent clients from assuming that the server is down.

Use the **radius-server deadtime** command to set an interval during which the access point does not attempt to use servers that do not respond, thus avoiding the wait for a request to time out before trying the next configured server. A server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to 1440 (24 hours).

This example shows how to set up two main servers and a local authenticator with a server deadtime of 10 minutes:

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654
AP(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337
AP(config)# radius-server deadtime 10
```

In this example, if the WAN link to the main servers fails, the access point completes these steps when a LEAP-enabled client device associates:

1. It tries the first server, times out multiple times, and marks the first server as dead.
2. It tries the second server, times out multiple times, and marks the second server as dead.
3. It tries and succeeds using the local authenticator.

If another client device needs to authenticate during the 10-minute dead-time interval, the access point skips the first two servers and tries the local authenticator first. After the dead-time interval, the access point tries to use the main servers for authentication. When setting a dead time, you must balance the need to skip dead servers with the need to check the WAN link and begin using the main servers again as soon as possible.

Each time the access point tries to use the main servers while they are down, the client device trying to authenticate might report an authentication timeout. The client device retries and succeeds when the main servers time out and the access point tries the local authenticator. You can extend the timeout value on Cisco client devices to accommodate expected server timeouts.

To remove the local authenticator from the access point configuration, use the **no radius-server host** ***hostname | ip-address*** global configuration command.

Unblocking Locked Usernames

You can unblock usernames before the lockout time expires, or when the lockout time is set to infinite. In Privileged Exec mode on the local authenticator, enter this command to unblock a locked username:

AP# clear radius local-server user *username*

Viewing Local Authenticator Statistics

In privileged exec mode, enter this command to view statistics collected by the local authenticator:

AP# show radius local-server statistics

This example shows local authenticator statistics:

```
Successes               : 0           Unknown usernames      : 0
Client blocks           : 0           Invalid passwords      : 0
Unknown NAS             : 0           Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes               : 0           Unknown usernames      : 0
Client blocks           : 0           Invalid passwords      : 0
Corrupted packet        : 0           Unknown RADIUS message : 0
No username attribute   : 0           Missing auth attribute : 0
Shared key mismatch     : 0           Invalid state attribute: 0
Unknown EAP message     : 0           Unknown EAP auth type  : 0

Username                   Successes  Failures  Blocks
nicky                              0         0       0
jones                              0         0       0
jsmith                             0         0       0
```

The first section of statistics lists cumulative stats from the local authenticator. The second section lists stats for each access point (NAS) authorized to use the local authenticator. The third section lists stats for individual users. If a user is blocked and the lockout time is set to infinite, *blocked* appears at the end of the stat line for that user. If the lockout time is not infinite, *Unblocked in x seconds* appears at the end of the stat line for that user.

Use this privileged exec mode command to reset local authenticator statistics to zero:

AP# clear radius local-server statistics

Using Debug Messages

In privileged exec mode, enter this command to control the display of debug messages for the local authenticator:

AP# debug radius local-server { **packets** | **error** | **client** }

Use the command options to display this debug information:

- Use the **packets** option to turn on display of the content of RADIUS packets sent and received.
- Use the **error** option to display error messages related to the local authenticator.
- Use the **client** option to display error messages related to failed client authentications.

Configuring Cipher Suites and WEP

This chapter describes how to configure the cipher suites required to use WPA and CCKM authenticated key management, Wired Equivalent Privacy (WEP), WEP features including Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), and broadcast key rotation. This chapter contains these sections:

- Understanding Cipher Suites and WEP, page 9-2
- Configuring Cipher Suites and WEP, page 9-3

Understanding Cipher Suites and WEP

This section describes how WEP and cipher suites protect traffic on your wireless LAN.

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point can receive the access point's radio transmissions. Because WEP is the first line of defense against intruders, Cisco recommends that you use full encryption on your wireless network.

WEP encryption scrambles the communication between the access point and client devices to keep the communication private. Both the access point and client devices use the same WEP key to encrypt and unencrypt radio signals. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to just one device on the network. Multicast messages are addressed to multiple devices on the network.

Extensible Authentication Protocol (EAP) authentication, also called 802.1x authentication, provides dynamic WEP keys to wireless users. Dynamic WEP keys are more secure than static, or unchanging, WEP keys. If an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join your network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key. See Chapter 10, "Configuring Authentication Types," for detailed information on EAP and other authentication types.

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM). Because cipher suites provide the protection of WEP while also allowing use of authenticated key management, Cisco recommends that you enable WEP by using the **encryption mode cipher** command in the CLI or by using the cipher drop-down menu in the web-browser interface. Cipher suites that contain TKIP provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

These security features protect the data traffic on your wireless LAN:

- AES-CCMP—Based on the Advanced Encryption Standard (AES) defined in the National Institute of Standards and Technology's *FIPS Publication 197*, AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.
- WEP (Wired Equivalent Privacy)—WEP is an 802.11 standard encryption algorithm originally designed to provide your wireless LAN with the same level of privacy available on a wired LAN. However, the basic WEP construction is flawed, and an attacker can compromise the privacy with reasonable effort.
- TKIP (Temporal Key Integrity Protocol)—TKIP is a suite of algorithms surrounding WEP that is designed to achieve the best possible security on legacy hardware built to run WEP. TKIP adds four enhancements to WEP:
  - A per-packet key mixing function to defeat weak-key attacks
  - A new IV sequencing discipline to detect replay attacks
  - A cryptographic message integrity Check (MIC), called *Michael*, to detect forgeries such as bit flipping and altering packet source and destination
  - An extension of IV space, to virtually eliminate the need for re-keying
- CKIP (Cisco Key Integrity Protocol)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
- CMIC (Cisco Message Integrity Check)—Like TKIP's *Michael*, Cisco's message integrity check mechanism is designed to detect forgery attacks.

- Broadcast key rotation (also known as Group Key Update)—Broadcast Key Rotation allows the access point to generate the best possible random group key and update all key-management capable clients periodically. Wi-Fi Protected Access (WPA) also provides additional options for group key updates. See the "Using WPA Key Management" section on page 10-7 for details on WPA.

Note Client devices using static WEP cannot use the access point when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

Configuring Cipher Suites and WEP

These sections describe how to configure cipher suites, WEP and additional WEP features such as MIC, TKIP, and broadcast key rotation:

- Creating WEP Keys, page 9-3
- Enabling Cipher Suites and WEP, page 9-6
- Enabling and Disabling Broadcast Key Rotation, page 9-7

Note WEP, TKIP, MIC, and broadcast key rotation are disabled by default.

Creating WEP Keys

Note You need to configure static WEP keys only if your access point needs to support client devices that use static WEP. If all the client devices that associate to the access point use key management (WPA, CCKM, or 802.1x authentication) you do not need to configure static WEP keys.

Beginning in privileged EXEC mode, follow these steps to create a WEP key and set the key properties:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	**encryption** [**vlan** *vlan-id*] **key** *1-4* **size** { **40** | **128** } *encryption-key* [**0** | **7**] [**transmit-key**]	Create a WEP key and set up its properties. • (Optional) Select the VLAN for which you want to create a key. • Name the key slot in which this WEP key resides. You can assign up to 4 WEP keys for each VLAN. • Enter the key and set the size of the key, either 40-bit or 128-bit. 40-bit keys contain 10 hexadecimal digits; 128-bit keys contain 26 hexadecimal digits. • (Optional) Specify whether the key is encrypted (**7**) or unencrypted (**0**). • (Optional) Set this key as the transmit key. The key in slot 1 is the transmit key by default. **Note** If you configure static WEP with MIC or CMIC, the access point and associated client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on the access point and the clients. **Note** Using security features such as authenticated key management can limit WEP key configurations. See the "WEP Key Restrictions" section on page 9-4 for a list of features that impact WEP keys.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to create a 128-bit WEP key in slot 3 for VLAN 22 and sets the key as the transmit key:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 key 3 size 128 12345678901234567890123456
transmit-key
ap1200(config-ssid)# end
```

WEP Key Restrictions

Table 9-1 lists WEP key restrictions based on your security configuration.

Table 9-1 WEP Key Restrictions

Security Configuration	WEP Key Restriction
CCKM or WPA authenticated key management	Cannot configure a WEP key in key slot 1
LEAP or EAP authentication	Cannot configure a WEP key in key slot 4
Cipher suite with 40-bit WEP	Cannot configure a 128-bit key
Cipher suite with 128-bit WEP	Cannot configure a 40-bit key
Cipher suite with TKIP	Cannot configure any WEP keys

Table 9-1 WEP Key Restrictions (continued)

Security Configuration	WEP Key Restriction
Cipher suite with TKIP and 40-bit WEP or 128-bit WEP	Cannot configure a WEP key in key slot 1 and 4
Static WEP with MIC or CMIC	Access point and client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on both access point and clients
Broadcast key rotation	Keys in slots 2 and 3 are overwritten by rotating broadcast keys **Note** Client devices using static WEP cannot use the access point when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

Example WEP Key Setup

Table 9-2 shows an example WEP key setup that would work for the access point and an associated device:

Table 9-2 WEP Key Setup Example

Key Slot	Access Point		Associated Device	
	Transmit?	Key Contents	Transmit?	Key Contents
1	x	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	x	09876543210987654321fedcba
3	—	not set	—	not set
4	—	not set	—	FEDCBA09876543211234567890

Because the access point's WEP key 1 is selected as the transmit key, WEP key 1 on the other device must have the same contents. WEP key 4 on the other device is set, but because it is not selected as the transmit key, WEP key 4 on the access point does not need to be set at all.

Note If you enable MIC but you use static WEP (you do not enable any type of EAP authentication), both the access point and any devices with which it communicates must use the same WEP key for transmitting data. For example, if the MIC-enabled access point uses the key in slot 1 as the transmit key, a client device associated to the access point must use the same key in its slot 1, and the key in the client's slot 1 must be selected as the transmit key.

Enabling Cipher Suites and WEP

Beginning in privileged EXEC mode, follow these steps to enable a cipher suite:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**encryption** [**vlan** *vlan-id*] **mode ciphers** {[**aes-ccm** | **ckip** | **cmic** | **ckip-cmic** | **tkip**]} {[**wep128** | **wep40**]}	Enable a cipher suite containing the WEP protection you need. Table 9-3 lists guidelines for selecting a cipher suite that matches the type of authenticated key management you configure. • (Optional) Select the VLAN for which you want to enable WEP and WEP features. • Set the cipher options and WEP level. You can combine TKIP with 128-bit or 40-bit WEP. **Note** If you enable a cipher suite with two elements (such as TKIP and 128-bit WEP), the second cipher becomes the group cipher. **Note** If you configure **ckip**, **cmic**, or **ckip-cmic**, you must also enable Aironet extensions. The command to enable Aironet extensions is **dot11 extension aironet**. **Note** You can also use the **encryption mode wep** command to set up static WEP. However, you should use **encryption mode wep** only if no clients that associate to the access point are capable of key management. See the *Cisco IOS Command Reference for Cisco Access Points and Bridges* for a detailed description of the **encryption mode wep** command. **Note** When you configure the cipher TKIP (not **TKIP + WEP 128** or **TKIP + WEP 40**) for an SSID, the SSID must use WPA or CCKM key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA or CCKM key management.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the encryption command to disable a cipher suite.

This example sets up a cipher suite for VLAN 22 that enables CKIP, CMIC, and 128-bit WEP.

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 mode ciphers ckip-cmic wep128
ap1200(config-if)# exit
```

Matching Cipher Suites with WPA and CCKM

If you configure your access point to use WPA or CCKM authenticated key management, you must select a cipher suite compatible with the authenticated key management type. Table 9-3 lists the cipher suites that are compatible with WPA and CCKM.

Table 9-3 Cipher Suites Compatible with WPA and CCKM

Authenticated Key Management Types	Compatible Cipher Suites
CCKM	• encryption mode ciphers wep128 • encryption mode ciphers wep40 • encryption mode ciphers ckip • encryption mode ciphers cmic • encryption mode ciphers ckip-cmic • encryption mode ciphers tkip
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40

Note When you configure the cipher TKIP (not **TKIP + WEP 128** or **TKIP + WEP 40**) for an SSID, the SSID must use WPA or CCKM key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA or CCKM key management.

For a complete description of WPA and CCKM and instructions for configuring authenticated key management, see the "Using CCKM for Authenticated Clients" section on page 10-6 and the "Using WPA Key Management" section on page 10-7.

Enabling and Disabling Broadcast Key Rotation

Broadcast key rotation is disabled by default.

Note Client devices using static WEP cannot use the access point when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

Beginning in privileged EXEC mode, follow these steps to enable broadcast key rotation:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	**broadcast-key change** *seconds* [**vlan** *vlan-id*] [**membership-termination**] [**capability-change**]	Enable broadcast key rotation. • Enter the number of seconds between each rotation of the broadcast key. • (Optional) Enter a VLAN for which you want to enable broadcast key rotation. • (Optional) If you enable WPA authenticated key management, you can enable additional circumstances under which the access point changes and distributes the WPA group key. – Membership termination—the access point generates and distributes a new group key when any authenticated client device disassociates from the access point. This feature protects the privacy of the group key for associated clients. However, it might generate some overhead if clients on your network roam frequently. – Capability change—the access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP clients associated to the access point. See Chapter 10, "Configuring Authentication Types," for detailed instructions on enabling authenticated key management.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the encryption command to disable broadcast key rotation.

This example enables broadcast key rotation on VLAN 22 and sets the rotation interval to 300 seconds:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# broadcast-key vlan 22 change 300
ap1200(config-ssid)# end
```

Configuring Authentication Types

This chapter describes how to configure authentication types on the access point. This chapter contains these sections:

- Understanding Authentication Types, page 10-2
- Configuring Authentication Types, page 10-10
- Matching Access Point and Client Device Authentication Types, page 10-17

Understanding Authentication Types

This section describes the authentication types that you can configure on the access point. The authentication types are tied to the SSIDs that you configure for the access point. If you want to serve different types of client devices with the same access point, you can configure multiple SSIDs. See Chapter 7, "Configuring Multiple SSIDs," for complete instructions on configuring multiple SSIDs.

Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point using open or shared-key authentication. For maximum security, client devices should also authenticate to your network using MAC-address or EAP authentication, authentication types that rely on an authentication server on your network.

Note By default, the access point sends reauthentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers do not support the authenticate-only service-type attribute. Changing the service-type attribute to login-only ensures that Microsoft IAS servers recognize reauthentication requests from the access point. Use the **dot11 aaa authentication attributes service-type login-only** global configuration command to set the service-type attribute in reauthentication requests to login-only.

The access point uses several authentication mechanisms or types and can use more than one at the same time. These sections explain each authentication type:

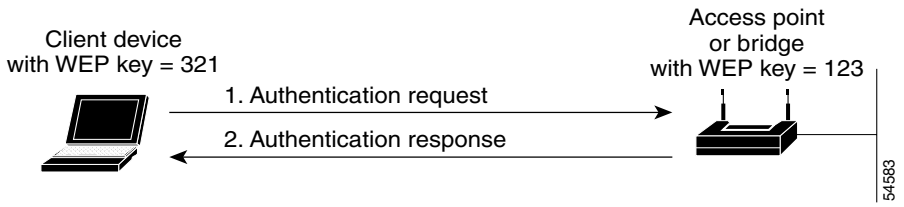
- Open Authentication to the Access Point, page 10-2
- Shared Key Authentication to the Access Point, page 10-3
- EAP Authentication to the Network, page 10-3
- MAC Address Authentication to the Network, page 10-5
- Combining MAC-Based, EAP, and Open Authentication, page 10-6
- Using CCKM for Authenticated Clients, page 10-6
- Using WPA Key Management, page 10-7

Open Authentication to the Access Point

Open authentication allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point, but the device can communicate only if its WEP keys match the access point's. Devices not using WEP do not attempt to authenticate with an access point that is using WEP. Open authentication does not rely on a RADIUS server on your network.

Figure 10-1 shows the authentication sequence between a device trying to authenticate and an access point using open authentication. In this example, the device's WEP key does not match the access point's key, so it can authenticate but not pass data.

Figure 10-1 Sequence for Open Authentication



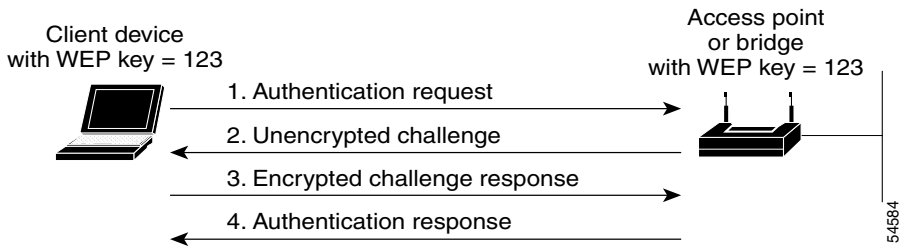
Shared Key Authentication to the Access Point

Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, Cisco recommends that you avoid using it.

During shared key authentication, the access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the access point open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network.

Figure 10-2 shows the authentication sequence between a device trying to authenticate and an access point using shared key authentication. In this example the device's WEP key matches the access point's key, so it can authenticate and communicate.

Figure 10-2 Sequence for Shared Key Authentication

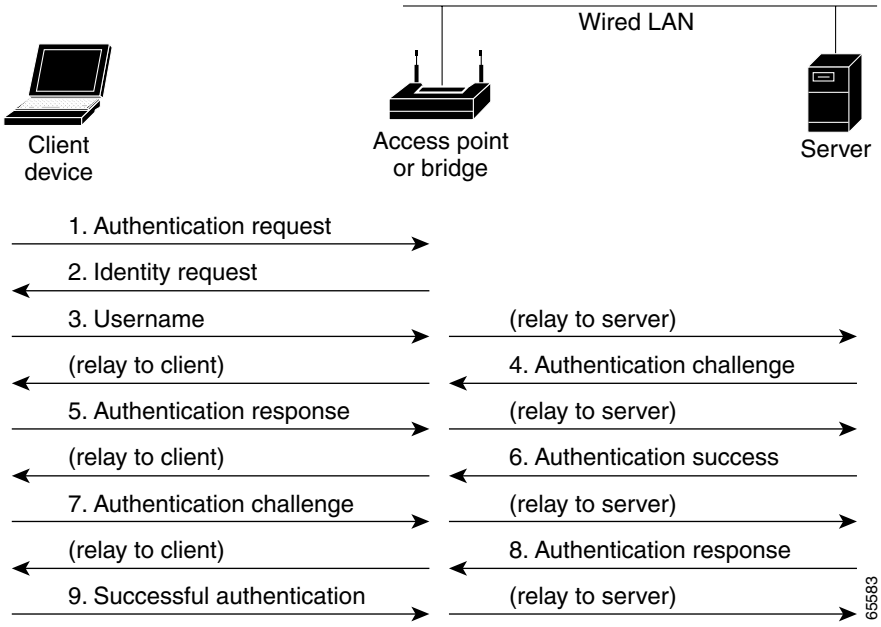


EAP Authentication to the Network

This authentication type provides the highest level of security for your wireless network. By using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. The RADIUS server sends the WEP key to the access point, which uses it for all unicast data signals that it sends to or receives from the client. The access point also encrypts its broadcast WEP key (entered in the access point's WEP key slot 1) with the client's unicast key and sends it to the client.

When you enable EAP on your access points and client devices, authentication to the network occurs in the sequence shown in Figure 10-3:

Figure 10-3 Sequence for EAP Authentication



In Steps 1 through 9 in Figure 10-3, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a WEP key that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the logon session.

During the logon session, the RADIUS server encrypts and sends the WEP key, called a *session key*, over the wired LAN to the access point. The access point encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the access point behaves the same way for each type: it relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the "Assigning Authentication Types to an SSID" section on page 10-10 for instructions on setting up EAP on the access point.

Note If you use EAP authentication, you can select open or shared key authentication, but you don't have to. EAP authentication controls authentication both to your access point and to your network.

MAC Address Authentication to the Network

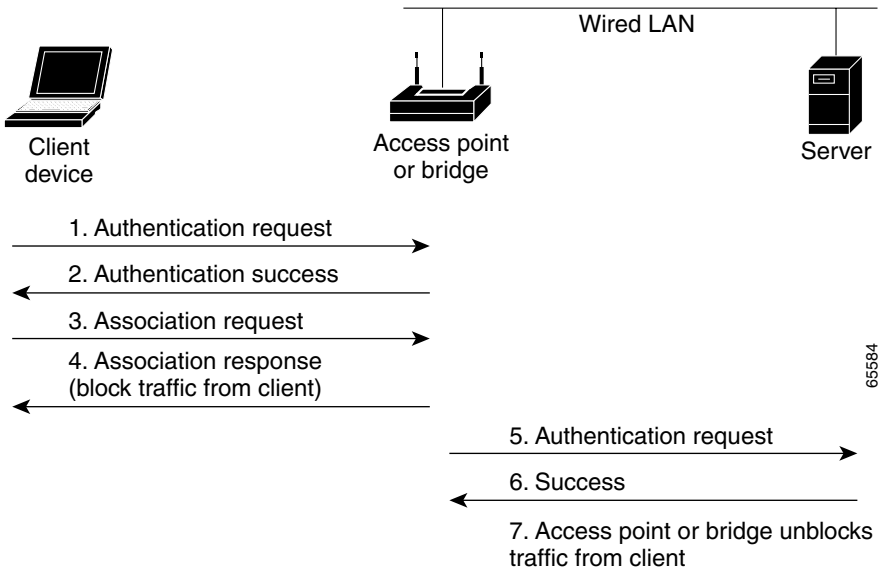
The access point relays the wireless client device's MAC address to a RADIUS server on your network, and the server checks the address against a list of allowed MAC addresses. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication. However, MAC-based authentication provides an alternate authentication method for client devices that do not have EAP capability. See the "Assigning Authentication Types to an SSID" section on page 10-10 for instructions on enabling MAC-based authentication.

Tip If you don't have a RADIUS server on your network, you can create a list of allowed MAC addresses on the access point's Advanced Security: MAC Address Authentication page. Devices with MAC addresses not on the list are not allowed to authenticate.

Tip If MAC-authenticated clients on your wireless LAN roam frequently, you can enable a MAC authentication cache on your access points. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. See the "Configuring MAC Authentication Caching" section on page 10-15 for instructions on enabling this feature.

Figure 10-4 shows the authentication sequence for MAC-based authentication.

Figure 10-4 Sequence for MAC-Based Authentication



Combining MAC-Based, EAP, and Open Authentication

You can set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication. When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. See the "Assigning Authentication Types to an SSID" section on page 10-10 for instructions on setting up this combination of authentications.

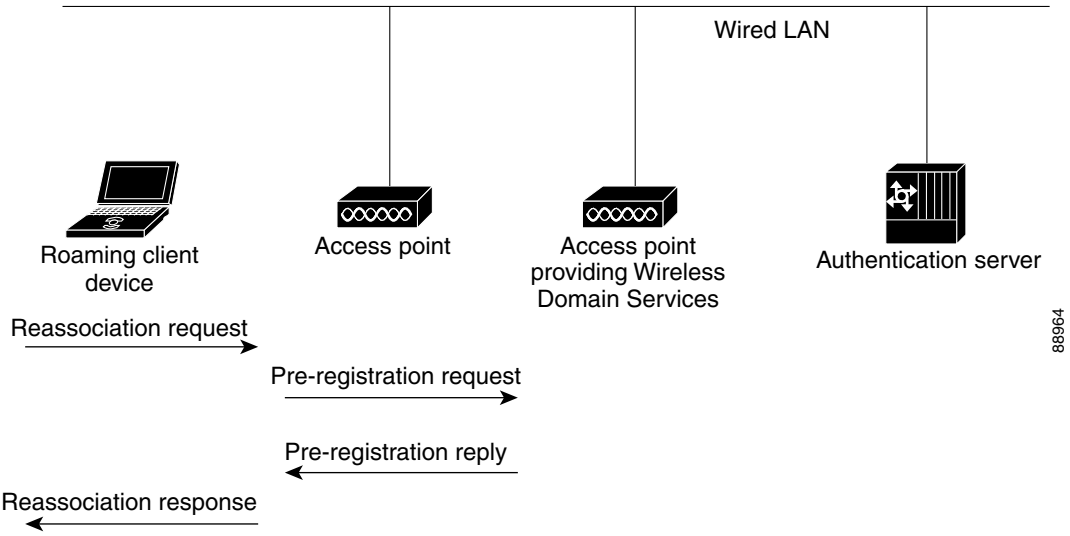
Using CCKM for Authenticated Clients

Using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. When a client device roams, the WDS access point forwards the client's security credentials to the new access point, and the reassociation process is reduced to a two-packet exchange between the roaming client and the new access point. Roaming clients reassociate so quickly that there is no perceptible delay in voice or other time-sensitive applications. See the "Assigning Authentication Types to an SSID" section on page 10-10 for instructions on enabling CCKM on your access point. See the "Configuring Access Points as Potential WDS Access Points" section on page 11-8 for detailed instructions on setting up a WDS access point on your wireless LAN.

Note The RADIUS-assigned VLAN feature is not supported for client devices that associate using SSIDs with CCKM enabled.

Figure 10-5 shows the reassociation process using CCKM.

Figure 10-5 Client Reassociation Using CCKM



Using WPA Key Management

Wi-Fi Protected Access is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

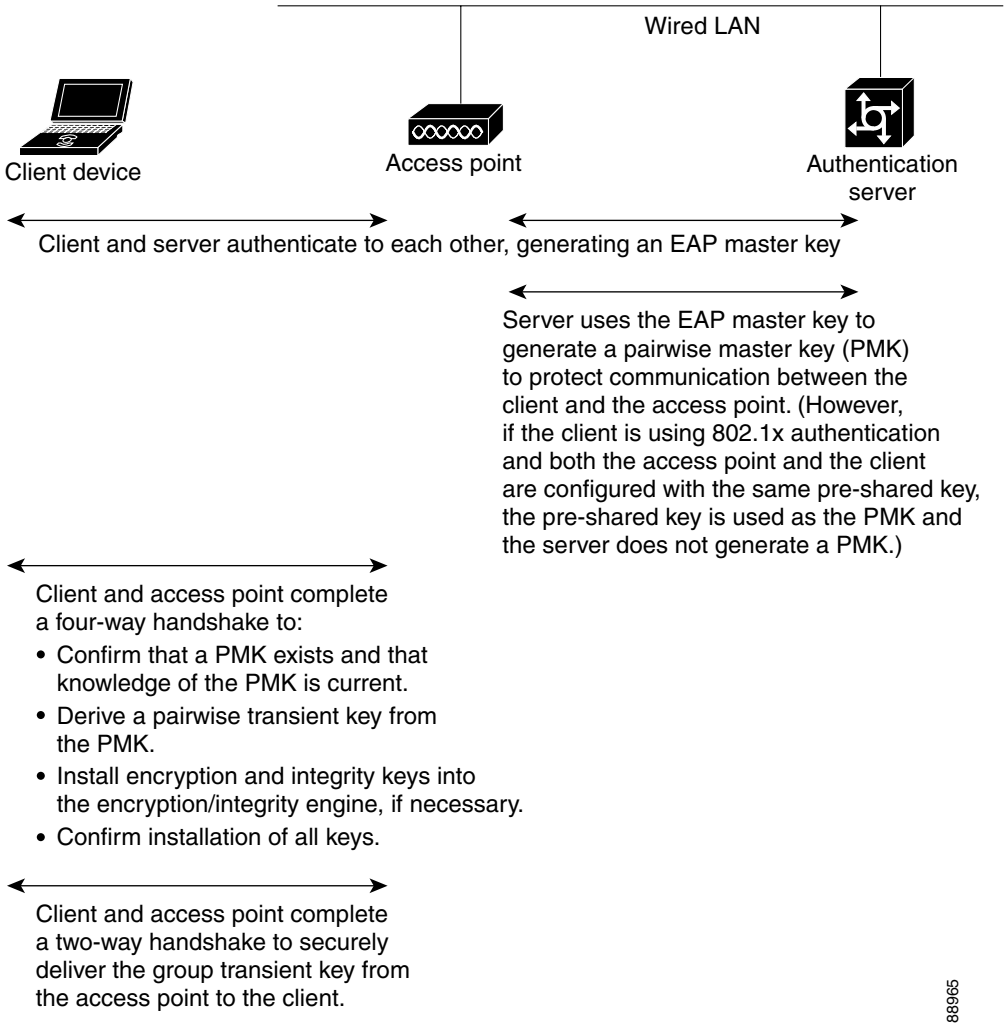
WPA key management supports two mutually exclusive management types: WPA and WPA-Pre-shared key (WPA-PSK). Using WPA key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the access point. Using WPA-PSK, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.

Note Unicast and multicast cipher suites advertised in WPA information element (and negotiated during 802.11 association) may potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new vlan ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the access point and client to switch back to the new cipher suite. Currently, the WPA and CCKM protocols do not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the client device is disassociated from the wireless LAN.

See the "Assigning Authentication Types to an SSID" section on page 10-10 for instructions on configuring WPA key management on your access point.

Figure 10-6 shows the WPA key management process.

Figure 10-6 WPA Key Management Process


Wired LAN
Client device
Access point
Authentication server
Client and server authenticate to each other, generating an EAP master key
Server uses the EAP master key to generate a pairwise master key (PMK) to protect communication between the client and the access point. (However, if the client is using 802.1x authentication and both the access point and the client are configured with the same pre-shared key, the pre-shared key is used as the PMK and the server does not generate a PMK.)
Client and access point complete a four-way handshake to:
• Confirm that a PMK exists and that knowledge of the PMK is current.
• Derive a pairwise transient key from the PMK.
• Install encryption and integrity keys into the encryption/integrity engine, if necessary.
• Confirm installation of all keys.
Client and access point complete a two-way handshake to securely deliver the group transient key from the access point to the client.
88965

Software and Firmware Requirements for WPA, CCKM, CKIP, and WPA-TKIP

Table 10-1 lists the firmware and software requirements required on access points and Cisco Aironet client devices to support WPA and CCKM key management and CKIP and WPA-TKIP encryption protocols.

To support the security combinations in Table 10-1, your Cisco Aironet access points and Cisco Aironet client devices must run the following software and firmware versions:

- Cisco IOS Release 12.2(13)JA or later on access points
- Install Wizard version 1.2 for 340, 350, and CB20A client devices, which includes these components:
  - PC, LM, and PCI card driver version 8.4
  - Mini PCI and PC-cardbus card driver version 3.7

- Aironet Client Utility (ACU) version 6.2
- Client firmware version 5.30.13

Table 10-1 Software and Firmware Requirements for WPA, CCKM, CKIP, and WPA-TKIP

Key Management and Encryption Protocol	Third Party Host Supplicant[1] Required?	Supported Platform Operating Systems
LEAP with CKIP **Note** This security combination requires 12.2(11)JA or later.	No	Windows 95/98, Me, NT, 2000, XP, Windows CE, Mac OS X, Linux, DOS
LEAP with CCKM and CKIP **Note** This security combination requires 12.2(11)JA or later.	No	Windows 98, Me, NT, 2000, XP, Windows CE
LEAP with CCKM and WPA-TKIP	No	Windows XP and 2000
LEAP with WPA (no CCKM)	No	Windows XP and 2000
Host-based EAP (such as PEAP, EAP-TLS, and EAP-SIM) with WPA (no CCKM)	No[2]	Windows XP
Host-based EAP (such as PEAP, EAP-TLS, and EAP-SIM) with WPA (no CCKM)	Yes	Windows 2000
WPA-PSK Mode	No[2]	Windows XP
WPA-PSK Mode	Yes	Windows 2000

1. Such as Funk Odyssey Client supplicant version 2.2 or Meetinghouse Data Communications Aegis Client version 2.1.
2. Windows XP does not require a third-party supplicant, but you must install Windows XP Service Pack 1 and Microsoft support patch 815485.

Refer to the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* for complete instructions on configuring security settings on Cisco Aironet client devices. Click this URL to browse to the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows*:

http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guides_list.html

Note When you configure **TKIP**-only cipher encryption (not **TKIP + WEP 128** or **TKIP + WEP 40**) on any radio interface or VLAN, every SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSIDs, client authentication fails on the SSIDs.

Configuring Authentication Types

This section describes how to configure authentication types. You attach configuration types to the access point's SSIDs. See Chapter 7, "Configuring Multiple SSIDs," for details on setting up multiple SSIDs. This section contains these topics:

- Default Authentication Settings, page 10-10
- Assigning Authentication Types to an SSID, page 10-10
- Configuring Authentication Holdoffs, Timeouts, and Intervals, page 10-16

Default Authentication Settings

The default SSID on the access point is *tsunami*. Table 10-2 shows the default authentication settings for the default SSID.

Table 10-2 Default Authentication Configuration

Feature	Default Setting
SSID	tsunami
Guest Mode SSID	tsunami (The access point broadcasts this SSID in its beacon and allows client devices with no SSID to associate.)

Assigning Authentication Types to an SSID

Beginning in privileged EXEC mode, follow these steps to configure authentication types for SSIDs:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. **Note** Do not include spaces in SSIDs.

	Command	Purpose
Step 4	**authentication open** [**mac-address** *list-name* [**alternate**]] [**eap** *list-name*]	(Optional) Set the authentication type to open for this SSID. Open authentication allows any device to authenticate and then attempt to communicate with the access point. • (Optional) Set the SSID's authentication type to open with MAC address authentication. The access point forces all client devices to perform MAC-address authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. Click this link for more information on method lists: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 Use the **alternate** keyword to allow client devices to join the network using either MAC or EAP authentication; clients that successfully complete either authentication are allowed to join the network. • (Optional) Set the SSID's authentication type to open with EAP authentication. The access point forces all client devices to perform EAP authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. **Note** An access point configured for EAP authentication forces all client devices that associate to perform EAP authentication. Client devices that do not use EAP cannot use the access point.
Step 5	**authentication shared** [**mac-address** *list-name*] [**eap** *list-name*]	(Optional) Set the authentication type for the SSID to shared key. **Note** Because of shared key's security flaws, Cisco recommends that you avoid using it. **Note** You can assign shared key athentication to only one SSID. • (Optional) Set the SSID's authentication type to shared key with MAC address authentication. For list-name, specify the authentication method list. • (Optional) Set the SSID's authentication type to shared key with EAP authentication. For list-name, specify the authentication method list.

	Command	Purpose
Step 6	**authentication network-eap** *list-name* [**mac-address** *list-name*]	(Optional) Set the authentication type for the SSID to Network-EAP. Using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. However, the access point does not force all client devices to perform EAP authentication. • (Optional) Set the SSID's authentication type to Network-EAP with MAC address authentication. All client devices that associate to the access point are required to perform MAC-address authentication. For list-name, specify the authentication method list.
Step 7	**authentication key-management** { [**wpa**] [**cckm**] } [**optional**]	(Optional) Set the authentication type for the SSID to WPA, CCKM, or both. If you use the **optional** keyword, client devices other than WPA and CCKM clients can use this SSID. If you do not use the **optional** keyword, only WPA or CCKM client devices are allowed to use the SSID. To enable CCKM for an SSID, you must also enable Network-EAP authentication. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both. **Note** When you enable both WPA and CCKM for an SSID, you must enter **wpa** first and **cckm** second. Any WPA client can attempt to authenticate, but only CCKM voice clients can attempt to authenticate. Only 802.11b and 802.11g radios support WPA and CCKM simultaneously. **Note** Before you can enable CCKM or WPA, you must set the encryption mode for the SSID's VLAN to one of the cipher suite options. To enable both CCKM and WPA, you must set the encryption mode to a cipher suite that includes TKIP. See the "Configuring Cipher Suites and WEP" section on page 9-3 for instructions on configuring the VLAN encryption mode. **Note** If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK. See the "Configuring Additional WPA Settings" section on page 10-14 for instructions on configuring a pre-shared key. See Chapter 11, "Configuring WDS, Fast Secure Roaming, and Radio Management," for detailed instructions on setting up your wireless LAN to use CCKM and a subnet context manager.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the SSID commands to disable the SSID or to disable SSID features.

This example sets the authentication type for the SSID *batman* to Network-EAP with CCKM authenticated key management. Client devices using the batman SSID authenticate using the adam server list. After they are authenticated, CCKM-enabled clients can perform fast reassociations using CCKM.

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management cckm optional
ap1200(config-ssid)# end
```

Configuring WPA Migration Mode

WPA migration mode allows these client device types to associate to the access point using the same SSID:

- WPA clients capable of TKIP and authenticated key management
- 802.1X-2001 clients (such as legacy LEAP clients and clients using TLS) capable of authenticated key management but not TKIP
- Static-WEP clients not capable of TKIP or authenticated key management

If all three client types associate using the same SSID, the multicast cipher suite for the SSID must be WEP. If only the first two types of clients use the same SSID the multicast key can be dynamic, but if the static-WEP clients use the SSID, the key must be static. The access point can switch automatically between a static and a dynamic group key to accommodate associated client devices. To support all three types of clients on the same SSID, you must configure the static key in key slots 2 or 3.

To set up an SSID for WPA migration mode, configure these settings:

- WPA optional
- A cipher suite containing TKIP and 40-bit or 128-bit WEP
- A static WEP key in key slot 2 or 3

This example sets the SSID migrate for WPA migration mode:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption mode cipher tkip wep128
ap1200(config-if)# encryption key 3 size 128 12345678901234567890123456 transmit-key
ap1200(config-if)# ssid migrate
ap1200(config-ssid)# authentication open
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management wpa optional
ap1200(config-ssid)# wpa-psk ascii batmobile65
ap1200(config-ssid)# exit
```

Configuring Additional WPA Settings

Use two optional settings to configure a pre-shared key on the access point and adjust the frequency of group key updates.

Setting a Pre-Shared Key

To support WPA on a wireless LAN where 802.1x-based authentication is not available, you must configure a pre-shared key on the access point. You can enter the pre-shared key as ASCII or hexadecimal characters. If you enter the key as ASCII characters, you enter between 8 and 63 characters, and the access point expands the key using the process described in the *Password-based Cryptography Standard* (RFC2898). If you enter the key as hexadecimal characters, you must enter 64 hexadecimal characters.

Configuring Group Key Updates

In the last step in the WPA process, the access point distributes a group key to the authenticated client device. You can use these optional settings to configure the access point to change and distribute the group key based on client association and disassociation:

- Membership termination—the access point generates and distributes a new group key when any authenticated device disassociates from the access point. This feature keeps the group key private for associated devices, but it might generate some overhead traffic if clients on your network roam frequently among access points.
- Capability change—the access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP clients associated to the access point.

Beginning in privileged EXEC mode, follow these steps to configure a WPA pre-shared key and group key update options:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**ssid** *ssid-string*	Enter SSID configuration mode for the SSID.
Step 4	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	Enter a pre-shared key for client devices using WPA that also use static WEP keys. Enter the key using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. You can enter a maximum of 63 ASCII characters.
Step 5	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 6	**broadcast-key** [**vlan** *vlan-id*] { **change** *seconds* } [**membership-termination**] [**capability-change**]	Use the **broadcast key rotation** command to configure additional updates of the WPA group key.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure a pre-shared key for clients using WPA and static WEP, with group key update options:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config-ssid)# exit
ap(config-if)# exit
ap(config)# broadcast-key vlan 87 membership-termination capability-change
```

Configuring MAC Authentication Caching

If MAC-authenticated clients on your wireless LAN roam frequently, you can enable a MAC authentication cache on your access points. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. When a client device completes MAC authentication to your authentication server, the access point adds the client's MAC address to the cache.

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication caching:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 aaa mac-authen filter-cache** [**timeout** *seconds*]	Enable MAC authentication caching on the access point. • Use the **timeout** option to configure a timeout value for MAC addresses in the cache. Enter a value from 30 to 65555 seconds. The default value is 1800 (30 minutes). When you enter a timeout value, MAC-authentication caching is enabled automatically.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show dot11 aaa mac-authen filter-cache** [*address*]	Show entries in the MAC-authentication cache. Include client MAC addresses to show entries for specific clients.
Step 5	**clear dot11 aaa mac-authen filter-cache** [*address*]	Clear all entries in the cache. Include client MAC addresses to clear specific clients from the cache.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the **dot11 aaa mac-authen filter-cache** command to disable MAC authentication caching. This example shows how to enable MAC authentication caching with a one-hour timeout:

```
ap# configure terminal
ap(config)# dot11 aaa mac-authen filter-cache timeout 3600
ap(config)# end
```

Configuring Authentication Holdoffs, Timeouts, and Intervals

Beginning in privileged EXEC mode, follow these steps to configure holdoff times, reauthentication periods, and authentication timeouts for client devices authenticating through your access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 holdoff-time** *seconds*	Enter the number of seconds a client device must wait before it can reattempt to authenticate following a failed authentication. The holdoff time is invoked when a client fails three login attempts or fails to respond to three authentication requests from the access point. Enter a value from 1 to 65555 seconds.
Step 3	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 4	**dot1x client-timeout** *seconds*	Enter the number of seconds the access point should wait for a reply from a client attempting to authenticate before the authentication fails. Enter a value from 1 to 65555 seconds.
Step 5	**dot1x reauth-period** { *seconds* | **server** }	Enter the interval in seconds that the access point waits before forcing an authenticated client to reauthenticate. Enter the **server** keyword to configure the access point to use the reauthentication period specified by the authentication server. If you use this option, configure your authentication server with RADIUS attribute 27, Session-Timeout. This attribute sets the maximum number of seconds of service to be provided to the client before termination of the session or prompt. The server sends this attribute to the access point when a client device performs EAP authentication. **Note** If you configure both MAC address authentication and EAP authentication for an SSID, the server sends the Session-Timeout attribute for both MAC and EAP authentications for a client device. The access point uses the Session-Timeout attribute for the last authentication that the client performs. For example, if a client performs MAC address authentication and then performs EAP authentication, the access point uses the server's Session-Timeout value for the EAP authentication. To avoid confusion on which Session-Timeout attribute is used, configure the same Session-Timeout value on your authentication server for both MAC and EAP authentication.

	Command	Purpose
Step 6	**countermeasure tkip hold-time** *seconds*	Configure a TKIP MIC failure holdtime. If the access point detects two MIC failures within 60 seconds, it blocks all the TKIP clients on that interface for the holdtime period.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of these commands to reset the values to default settings.

Matching Access Point and Client Device Authentication Types

To use the authentication types described in this section, the access point authentication settings must match the authentication settings on the client adapters that associate to the access point. Refer to the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows* for instructions on setting authentication types on wireless client adapters. Refer to Chapter 9, "Configuring Cipher Suites and WEP," for instructions on configuring cipher suites and WEP on the access point.

Table 10-3 lists the client and access point settings required for each authentication type.

Note Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

Table 10-3 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication for the SSID
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP for the SSID[1]
EAP-FAST authentication	Enable EAP-FAST and enable automatic provisioning or import a PAC file	Set up and enable WEP and enable Network-EAP for the SSID[1]

Table 10-3 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
EAP-FAST authentication with WPA	Enable EAP-FAST and Wi-Fi Protected Access (WPA) and enable automatic provisioning or import a PAC file. To allow the client to associate to both WPA and non-WPA access points, enable Allow Association to both WPA and non-WPA authenticators.	Select a cipher suite that includes TKIP, set up and enable WEP, and enable Network-EAP and WPA for the SSID. **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
802.1x authentication and CCKM	Enable LEAP	Select a cipher suite and enable Network-EAP and CCKM for the SSID **Note** To allow both 802.1x clients and non-802.1x clients to use the SSID, enable optional CCKM.
802.1x authentication and WPA	Enable any 802.1x authentication method	Select a cipher suite and enable Open authentication and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication) **Note** To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
802.1x authentication and WPA-PSK	Enable any 802.1x authentication method	Select a cipher suite and enable Open authentication and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication). Enter a WPA pre-shared key. **Note** To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.

Table 10-3 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
EAP-TLS authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and Smart Card or Other Certificate as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP and enable EAP and Open authentication for the SSID
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type	Set up and enable WEP and enable EAP and Open Authentication for the SSID
EAP-MD5 authentication		
If using ACU to configure card	Create a WEP key, enable Host Based EAP, and enable Use Static WEP Keys in ACU and select Enable network access control using IEEE 802.1X and MD5-Challenge as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP and enable EAP and Open authentication for the SSID
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and MD5-Challenge as the EAP Type	Set up and enable WEP and enable EAP and Open Authentication for the SSID
PEAP authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and PEAP as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP and enable EAP and Open authentication for the SSID
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and PEAP as the EAP Type	Set up and enable WEP and enable Require EAP and Open Authentication for the SSID

Table 10-3 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
EAP-SIM authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and SIM Authentication as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP with full encryption and enable EAP and Open authentication for the SSID
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and SIM Authentication as the EAP Type	Set up and enable WEP with full encryption and enable Require EAP and Open Authentication for the SSID

1. Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

CHAPTER 11

Configuring WDS, Fast Secure Roaming, and Radio Management

This chapter describes how to configure your access points for wireless domain services (WDS), fast, secure roaming of client devices, and radio management. This chapter contains these sections:

- Understanding WDS, page 11-2
- Understanding Fast Secure Roaming, page 11-3
- Understanding Radio Management, page 11-4
- Understanding Layer 3 Mobility, page 11-4
- Configuring WDS and Fast Secure Roaming, page 11-6
- Configuring Radio Management, page 11-23

Understanding WDS

When you configure Wireless Domain Services on your network, access points on your wireless LAN use the WDS device (either an access point or a switch configured as the WDS device) to provide fast, secure roaming for client devices and to participate in radio management. If you use a switch as the WDS device, the switch must be equipped with a Wireless LAN Services Module (WLSM). An access point configured as the WDS device supports up to 60 participating access points. A WLSM-equipped switch supports up to 300 participating access points.

Fast, secure roaming provides rapid reauthentication when a client device roams from one access point to another, preventing delays in voice and other time-sensitive applications.

Access points participating in radio management forward information about the radio environment (such as possible rogue access points and client associations and disassociations) to the WDS device. The WDS device aggregates the information and forwards it to a wireless LAN solution engine (WLSE) device on your network.

Role of the WDS Device

The WDS device performs several tasks on your wireless LAN:

- Advertises its WDS capability and participates in electing the best WDS device for your wireless LAN. When you configure your wireless LAN for WDS, you set up one device as the main WDS candidate and one or more additional devices as backup WDS candidates. If the main WDS device goes off line, one of the backup WDS devices takes its place.
- Authenticates all access points in the subnet and establishes a secure communication channel with each of them.
- Collects radio data from access points in the subnet, aggregates the data, and forwards it to the WLSE device on your network.
- Registers all client devices in the subnet, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS device forwards the client's security credentials to the new access point.

Table 11-1 lists the number of participating access points supported by an acess point configured as the WDS device and by a WLSM-equipped switch configured as the WDS device.

Table 11-1 Participating Access Points Supported by WDS Devices

Unit Configured as WDS Device	Participating Access Points Supported
Access point that also serves client devices	30
Access point with radio interfaces disabled	60
WLSM-equipped switch	300

Role of Access Points Using the WDS Device

The access points on your wireless LAN interact with the WDS device in these activities:

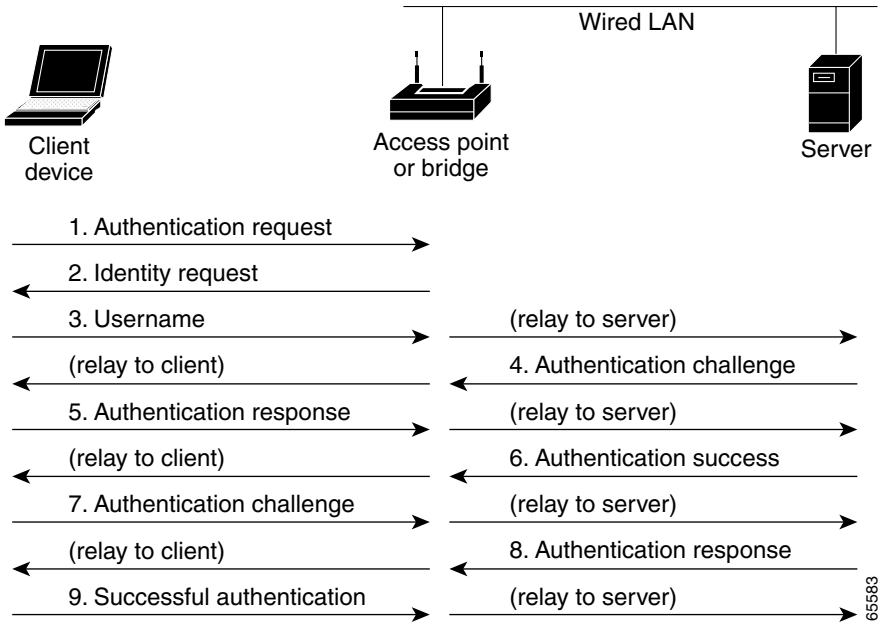
- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.
- Report radio data to the WDS device.

Understanding Fast Secure Roaming

Access points in many wireless LANs serve mobile client devices that roam from access point to access point throughout the installation. Some applications running on client devices require fast reassociation when they roam to a different access point. Voice applications, for example, require seamless roaming to prevent delays and gaps in conversation.

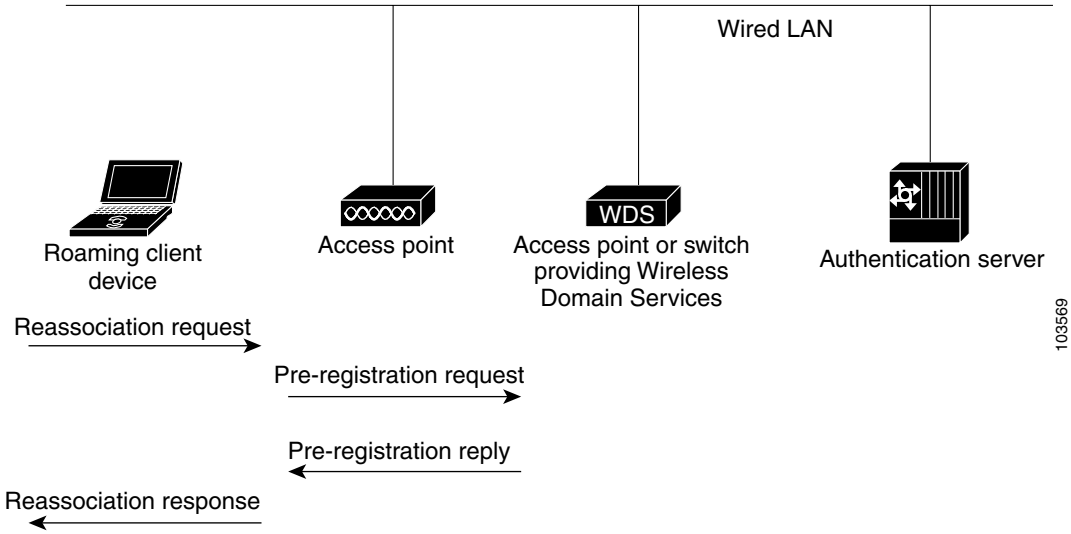
During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server, as in Figure 11-1.

Figure 11-1 Client Authentication Using a RADIUS Server



When you configure your wireless LAN for fast, secure roaming, however, LEAP-enabled client devices roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), a device configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications. Figure 11-2 shows client authentication using CCKM.

Figure 11-2 Client Reassociation Using CCKM and a WDS Access Point



The WDS device maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the client sends a reassociation request to the new access point, and the new access point relays the request to the WDS device. The WDS device forwards the client's credentials to the new access point, and the new access point sends the reassociation response to the client. Only two packets pass between the client and the new access point, greatly shortening the reassociation time. The client also uses the reassociation response to generate the unicast key.

Understanding Radio Management

Access points participating in radio management scan the radio environment and send reports to the WDS device on such radio information as potential rogue access points, associated clients, client signal strengths, and the radio signals from other access points. The WDS device forwards the aggregated radio data to the WLSE device on your network. Access points participating in radio management also assist with the self-healing wireless LAN, automatically adjusting settings to provide coverage in case a nearby access point fails. Refer to the "Configuring Radio Management" section on page 11-23 for instructions on configuring radio management.

Understanding Layer 3 Mobility

When you use a WLSM as the WDS device on your network, you can install access points anywhere in a large Layer 3 network without configuring one specific subnet or VLAN throughout the wired switch infrastructure. Client devices use multipoint GRE (mGRE) tunnels to roam to access points that reside on different Layer 3 subnets. The roaming clients stay connected to your network without changing IP addresses.

The access point features that provide mobile clients with fast, secure Layer 3 mobility are IP-Based Wireless Domain Services and Layer 3 Mobility Service Through Fast Secure Roaming Tunnels.

IP-Based Wireless Domain Services

You use IP-based WDS to configure the access point with the IP address of its WDS device. This allows the access point to use a Cisco network infrastructure device running WDS from anywhere in the network.

Layer 3 Mobility Service Through Fast Secure Roaming Tunnels

The access point uses this feature to segregate WLAN clients into different mobility groups. After a client is authenticated according to its mobility group's security policy, all IP traffic from that client is encapsulated using generic routing encapsulation (GRE) and sent to a specific multipoint GRE (mGRE) interface of a Cisco Structured Wireless-Aware Network (SWAN) infrastructure device that supports mobility groups. An access point with Layer 3 Mobility Service provides clients within each mobility group with Layer 3 mobility when used with a Cisco SWAN infrastructure device supporting Layer 3 mobility. Support for Layer 3 roaming is provided for all Wi-Fi certified client devices. Support for fast secure Layer 3 roaming is provided for Cisco or Cisco Compatible wireless LAN client devices using the Cisco Centralized Key Management (CCKM) protocol.

Components Required for Layer 3 Mobility

The Layer 3 mobility wireless LAN solution consists of these hardware and software components:

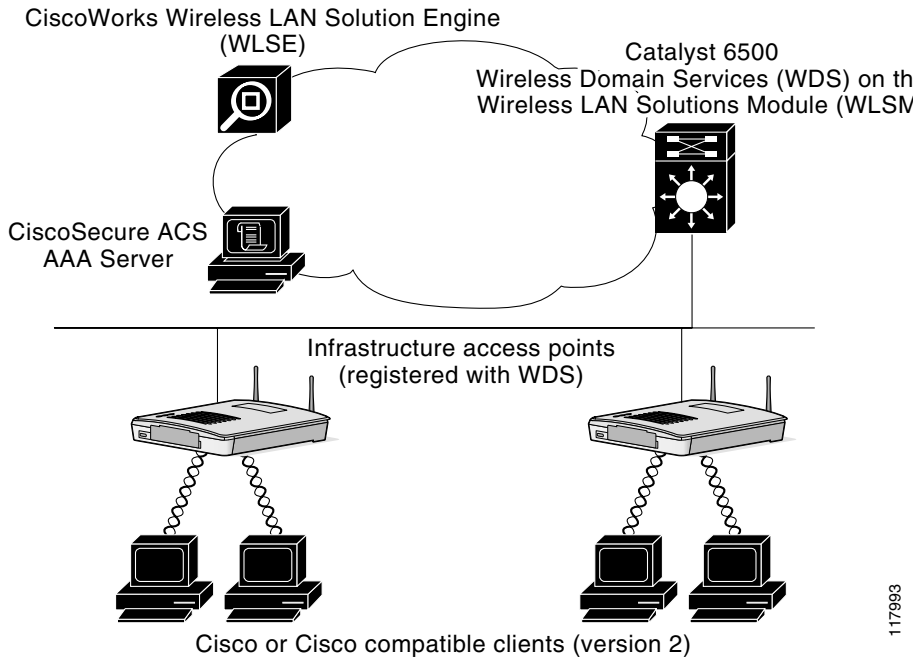
- 1100 or 1200 series access points participating in WDS
- Catalyst 6500 switch with Supervisor Module and WLSM configured as the WDS device

Note You must use a WLSM as your WDS device to properly configure Layer 3 mobility. Layer 3 mobility is not supported when your WDS device is an access point.

- Cisco (or Cisco compatible) client devices

Figure 11-3 shows the components that interact to perform Layer 3 mobility.

Figure 11-3 Required Components for Layer 3 Mobility



Configuring WDS on the WLSM

For instructions on configuring WDS on a switch's Wireless LAN Services Module (WLSM), refer to the *Catalyst 6500 Series Wireless LAN Services Module Installation and Configuration Note*.

Click this link to browse to the information pages for the Cisco Structured Wireless-Aware Network (SWAN):

http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html

Configuring WDS and Fast Secure Roaming

This section describes how to configure WDS on your network and fast, secure roaming on your wireless LAN. This section contains these sections:

- Guidelines for WDS, page 11-7
- Requirements for WDS and Fast Secure Roaming, page 11-7
- Configuration Overview, page 11-7
- Configuring Access Points as Potential WDS Access Points, page 11-8
- Configuring Access Points to use the WDS Device, page 11-13
- Configuring the Authentication Server to Support Fast Secure Roaming, page 11-15
- Viewing WDS Information, page 11-21
- Using Debug Messages, page 11-22

Guidelines for WDS

Follow these guidelines when configuring WDS:

- If you use an access point as your WDS device, either disable the radio interfaces on the unit or use an access point that does not serve a large number of client devices. If client devices associate to the WDS access point when it starts up, the clients might wait up to 10 minutes to be authenticated.
- A WDS access point that also serves client devices supports up to 30 participating access points, but a WDS access point with radios disabled supports up to 60 participating access points.
- Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to return (fall back) to repeater mode in case of Ethernet failure.
- You cannot configure a 350 series access point as a WDS access point. However, you can configure 350 series access points to use the WDS access point.

Requirements for WDS and Fast Secure Roaming

To configure WDS, you must have these items on your wireless LAN:

- At least one access point or switch (equipped with a Wireless LAN Services Module) that you can configure as the WDS device
- An authentication server (or an access point configured as a local authenticator)
- Cisco Aironet client devices running Cisco client firmware version 5.20.17 or later

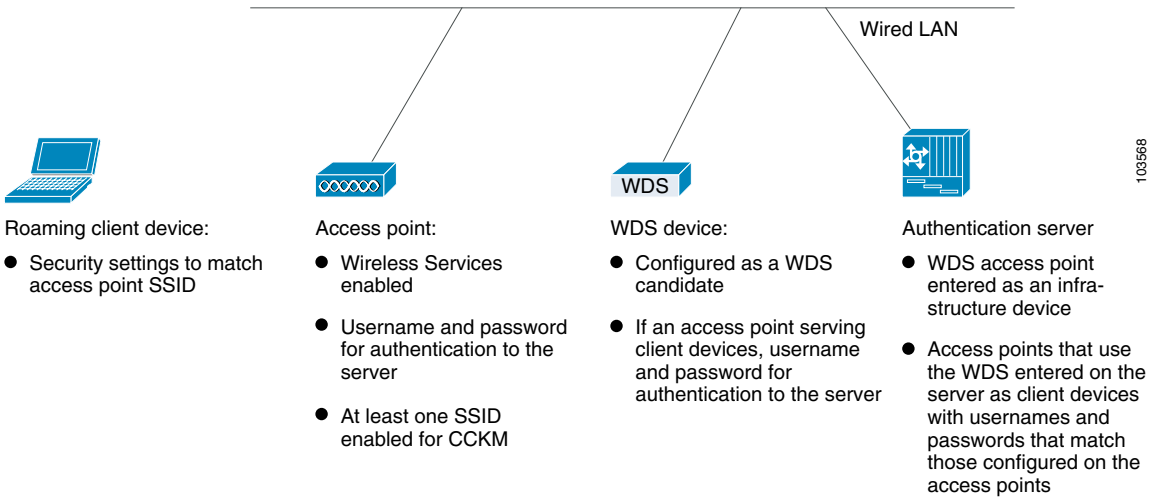
Configuration Overview

You must complete three major steps to set up WDS and fast, secure roaming:

1. Configure access points or switches as potential WDS devices. This chapter provides instructions for configuring an access point as a WDS device. For instructions on configuring a WLSM-equipped switch as a WDS device, refer to the *Catalyst 6500 Series Wireless LAN Services Module Installation and Configuration Note*.
2. Configure the rest of your access points to use the WDS device.
3. Enable access points on the subnet to allow CCKM authenticated key management for at least one SSID. See the "Configuring Authentication Types" section on page 10-10 for complete instructions on enabling CCKM.
4. Configure the authentication server on your network to authenticate the WDS device and the access points that use the WDS device.

Figure 11-4 shows the required configuration for each device that participates in fast, secure roaming.

Figure 11-4 Configurations on Devices Participating in WDS and CCKM


Wired LAN
WDS
103568
Roaming client device:
Security settings to match access point SSID
Access point:
Wireless Services enabled
Username and password for authentication to the server
At least one SSID enabled for CCKM
WDS device:
Configured as a WDS candidate
If an access point serving client devices, username and password for authentication to the server
Authentication server
WDS access point entered as an infra-structure device
Access points that use the WDS entered on the server as client devices with usernames and passwords that match those configured on the access points

Configuring Access Points as Potential WDS Access Points

Note For the main WDS candidate, configure an access point that does not serve a large number of client devices. If client devices associate to the WDS access point when it starts up, the clients might wait up to 10 minutes to be authenticated.

Note Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.

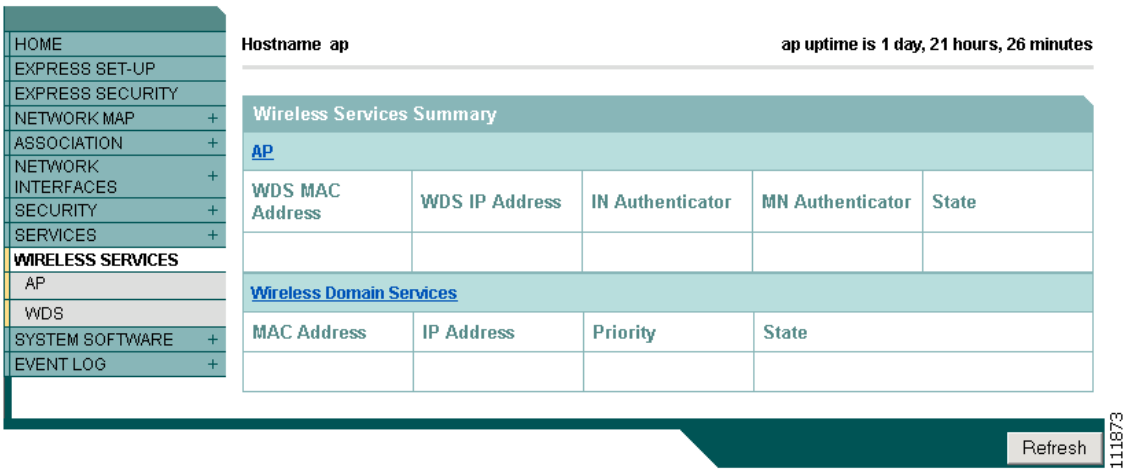
Note When WDS is enabled, the WDS access point performs and tracks all LEAP authentications. Therefore, you must configure EAP security settings on the WDS access point. See Chapter 10, "Configuring Authentication Types," for instructions on configuring EAP on the access point.

Note You cannot configure a 350 series access point as a WDS access point. However, you can configure 350 series access points to participate in WDS through the WDS device on your network.

On the access point that you want to configure as your primary WDS access point, follow these steps to configure the access point as the main WDS candidate:

Step 1 Browse to the Wireless Services Summary page. Figure 11-5 shows the Wireless Services Summary page.

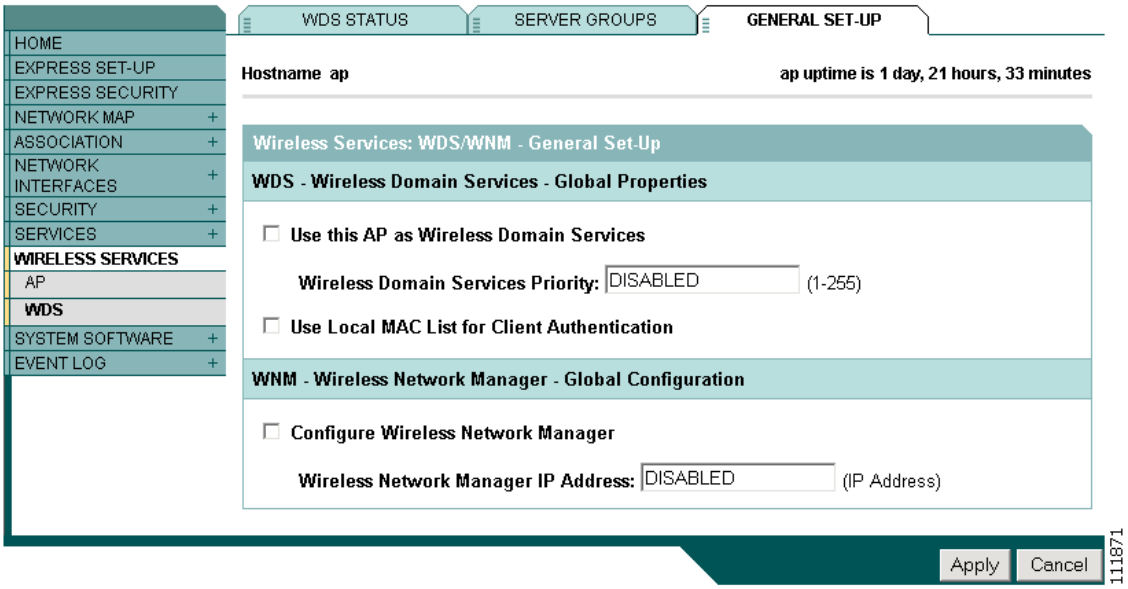
Figure 11-5 Wireless Services Summary Page



Step 2 Click **WDS** to browse to the WDS/WNM Summary page.

Step 3 On the WDS/WNM Summary page, click **General Setup** to browse to the WDS/WNM General Setup page. Figure 11-6 shows the General Setup page.

Figure 11-6 WDS/WNM General Setup Page



Step 4 Check the *Use this AP as Wireless Domain Services* check box.

Step 5 In the Wireless Domain Services Priority field, enter a priority number from 1 to 255 to set the priority of this WDS candidate. The WDS access point candidate with the highest number in the priority field becomes the acting WDS access point. For example, if one WDS candidate is assigned priority 255 and one candidate is assigned priority 100, the candidate with priority 255 becomes the acting WDS access point.

Step 6 (Optional) Select the *Use Local MAC List for Client Authentication* check box to authenticate client devices using MAC addresses in the local list of addresses configured on the WDS device. If you do not select this check box, the WDS device uses the server specified for MAC-address authentication on the Server Groups page to authenticate clients based on MAC addresses.

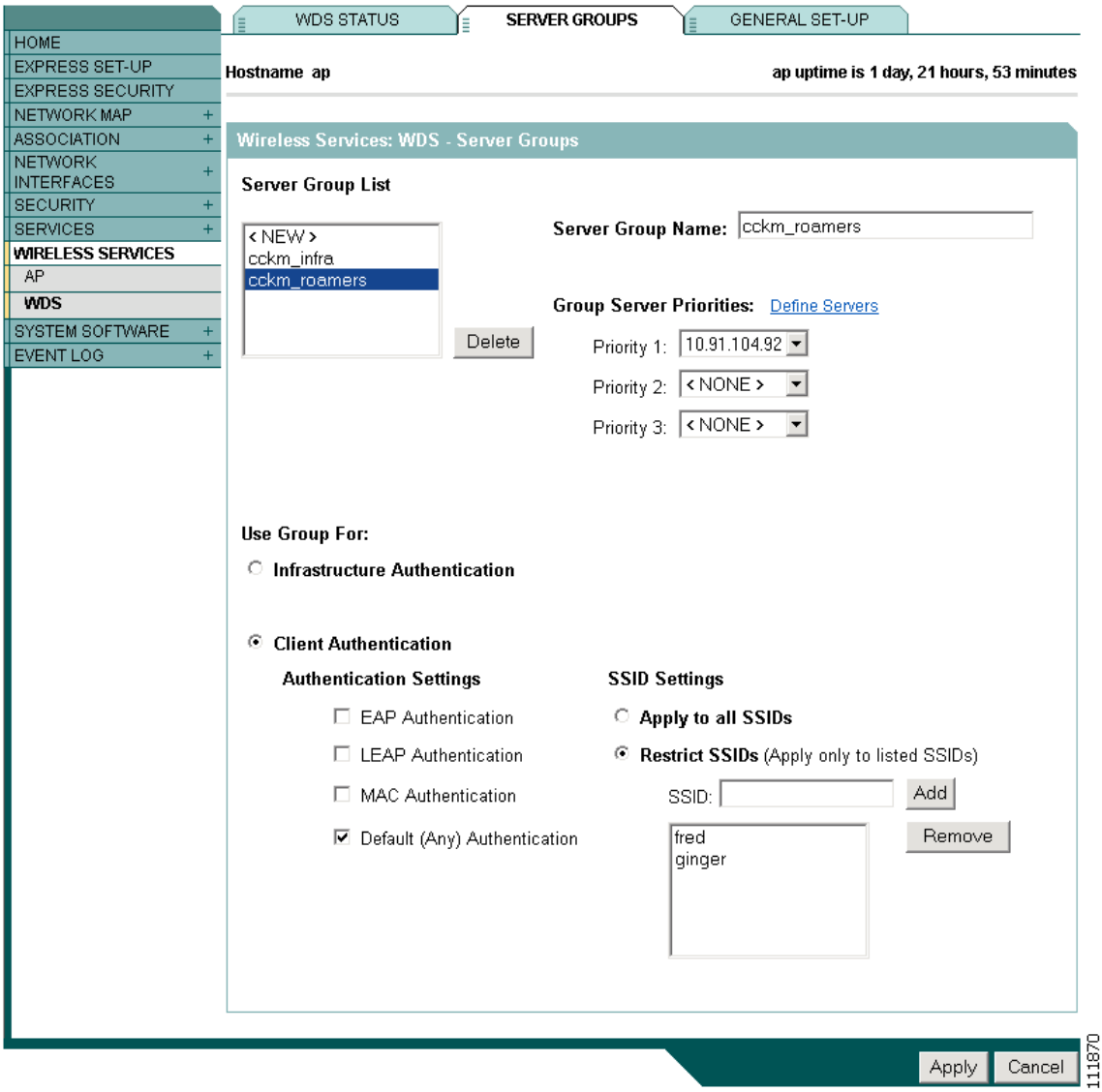
Note Selecting the *Use Local MAC List for Client Authentication* check box does not force client devices to perform MAC-based authentication. It provides a local alternative to server-based MAC-address authentication.

Step 7 (Optional) If you use a Wireless LAN Solutions Engine (WLSE) on your network, check the *Configure Wireless Network Manager* check box and enter the IP address of the WLSE device in the *Wireless Network Manager IP Address* field. The WDS access point collects radio measurement information from access points and client devices and sends the aggregated data to the WLSE device.

Step 8 Click **Apply**.

Step 9 Click **Server Groups** to browse to the WDS Server Groups page. Figure 11-7 shows the WDS Server Groups page.

Figure 11-7 WDS Server Groups Page



Step 10 Create a group of servers to be used for 802.1x authentication for the infrastructure devices (access points) that use the WDS access point. Enter a group name in the Server Group Name field.

Step 11 Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)

Note If you don't have an authentication server on your network, you can configure an access point as a local authentication server. See Chapter 8, "Configuring an Access Point as a Local Authenticator," for configuration instructions.

Step 12 (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.

Step 13 Click **Apply**.

Step 14 Configure the list of servers to be used for 802.1x authentication for CCKM-enabled client devices. You can specify a separate list for clients using a certain type of authentication, such as EAP, LEAP, or MAC-based, or specify a list for client devices using any type of authentication. Enter a group name for the server or servers in the Server Group Name field.

Step 15 Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)

Step 16 (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.

Step 17 (Optional) Select **Restrict SSIDs** to limit use of the server group to client devices using specific SSIDs. Enter an SSID in the SSID field and click **Add**. To remove an SSID, highlight it in the SSID list and click **Remove**.

Step 18 Click **Apply**.

Step 19 Configure the WDS access point for LEAP authentication. See Chapter 10, "Configuring Authentication Types," for instructions on configuring LEAP.

Note If your WDS access point serves client devices, follow the instructions in the "Configuring Access Points to use the WDS Device" section on page 11-13 to configure the WDS access point to use the WDS.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Access Points as Potential WDS Access Points" section on page 11-8:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server infrastructure cckm_infra
AP(config)# wlccp authentication-server client any cckm_roamers
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

In this example, infrastructure devices are authenticated using server group *cckm_infra*; CCKM-enabled client devices using SSIDs *fred* or *ginger* are authenticated using server group *cckm_roamers*.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

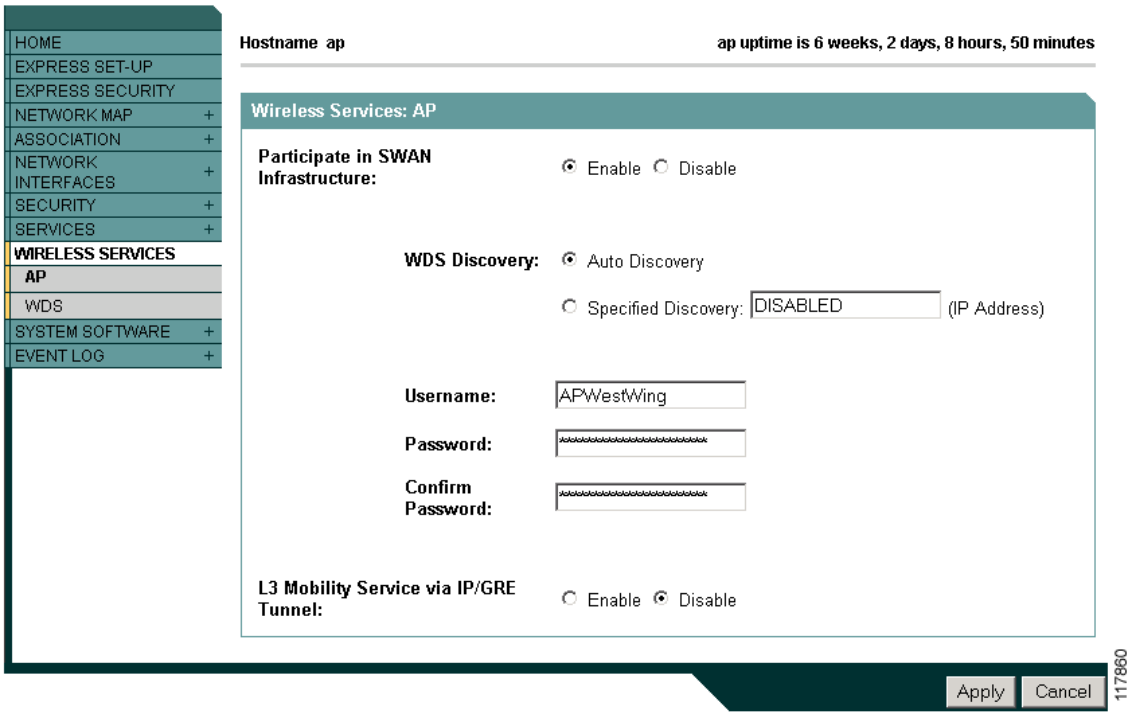
Configuring Access Points to use the WDS Device

Follow these steps to configure an access point to authenticate through the WDS device and participate in CCKM:

Step 1 Browse to the Wireless Services Summary page.

Step 2 Click **AP** to browse to the Wireless Services AP page. Figure 11-8 shows the Wireless Services AP page.

Figure 11-8 Wireless Services AP Page



Step 3 Click **Enable** for the *Participate in SWAN Infrastructure* setting.

Step 4 (Optional) Select **Specified Discovery** and enter the IP address of the WDS device in the entry field. This feature--IP-based WDS--allows the access point to use a Cisco network infrastructure device running WDS from anywhere in the network. When you enable Specified Discovery, the access point immediately authenticates with the WDS device instead of waiting for WDS advertisements. If the WDS device that you specify does not respond, the access point waits for WDS advertisements.

Step 5 In the Username field, enter a username for the access point. This username must match the username that you create for the access point on your authentication server.

Step 6 In the Password field, enter a password for the access point, and enter the password again in the Confirm Password field. This password must match the password that you create for the access point on your authentication server.

Step 7 (Optional) Select **Enable** for the L3 Mobility Service via IP/GRE Tunnel setting to configure the access point to participate in Layer 3 mobility. Your wireless LAN must contain these components to enable Layer 3 mobility:

- 1100 or 1200 series access points participating in WDS
- a Cisco Catalyst 6500 switch equipped with a WLSM configured as the WDS device

Note The **L3 Mobility Service via IP/GRE Tunnel** option does not appear on the Wireless Services AP page on access points running Cisco IOS Release 12.2(15)XR or later. This feature is enabled automatically on access points running Cisco IOS Release 12.2(15)XR or later.

Step 8 Click **Apply**.

The access points that you configure to interact with the WDS automatically perform these steps:

- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Access Points to use the WDS Device" section on page 11-13:

```
AP# configure terminal
AP(config)# wlccp ap wds ip address 10.91.104.92
AP(config)# wlccp ap username APWestWing password 7 wes7win8
AP(config)# end
```

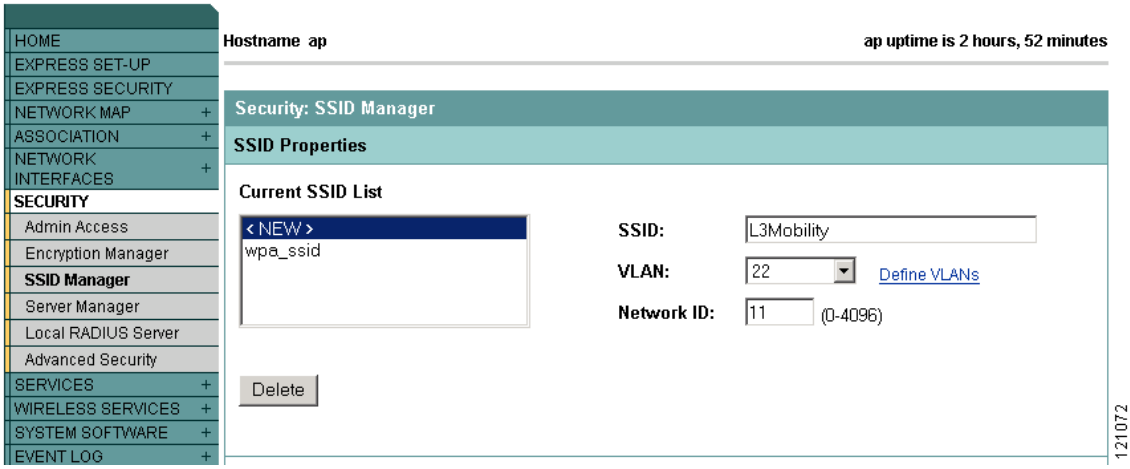
In this example, the access point is enabled to interact with a specific WDS device, and it authenticates to the authentication server using *APWestWing* as its username and *wes7win8* as its password. You must configure the same username and password pair when you set up the access point as a client on your authentication server.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Enabling Layer 3 Mobility on an SSID

Use the Network ID entry field on the SSID Manager page to map an SSID to a specific mobility network ID. Figure 11-9 shows the SSID Manager page.

Figure 11-9 Network ID Entry Field on the SSID Manager Page



CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Enabling Layer 3 Mobility on an SSID" section on page 11-15:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid L3Mobility
AP(config-if-ssid)# mobility network-id 11
AP(config-if-ssid)# end
```

In this example, the SSID *L3Mobility* is mapped to mobility network ID 11.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

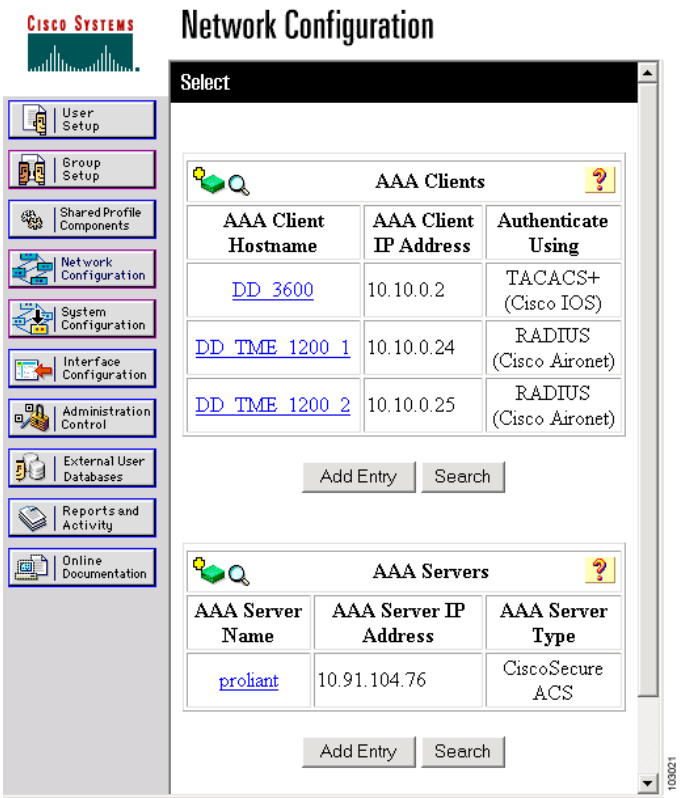
Configuring the Authentication Server to Support Fast Secure Roaming

The WDS device and all access points participating in CCKM must authenticate to your authentication server. On your server, you must configure usernames and passwords for the access points and a username and password for the WDS device.

If your server runs Cisco ACS, follow these steps to configure the access points on your server:

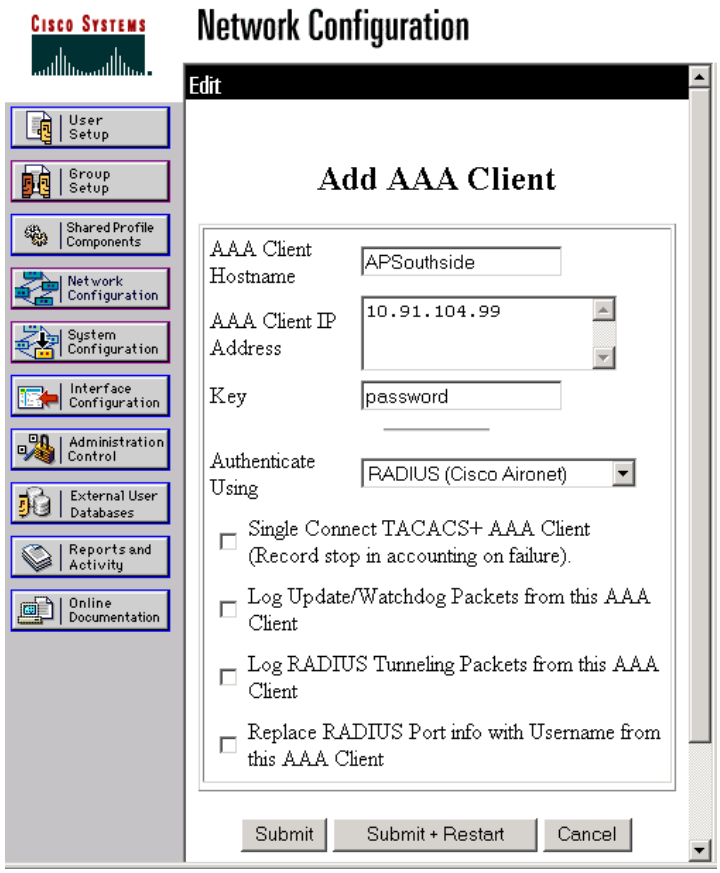
Step 1 Log into Cisco Secure ACS and click **Network Configuration** to browse to the Network Configuration page. You must use the Network Configuration page to create an entry for the WDS device. Figure 11-10 shows the Network Configuration page.

Figure 11-10 Network Configuration Page



Step 2 Click **Add Entry** under the AAA Clients table. The Add AAA Client page appears. Figure 11-11 shows the Add AAA Client page.

Figure 11-11 Add AAA Client Page



Step 3 In the AAA Client Hostname field, enter the name of the WDS device.

Step 4 In the AAA Client IP Address field, enter the IP address of the WDS device.

Step 5 In the Key field, enter exactly the same password that is configured on the WDS device.

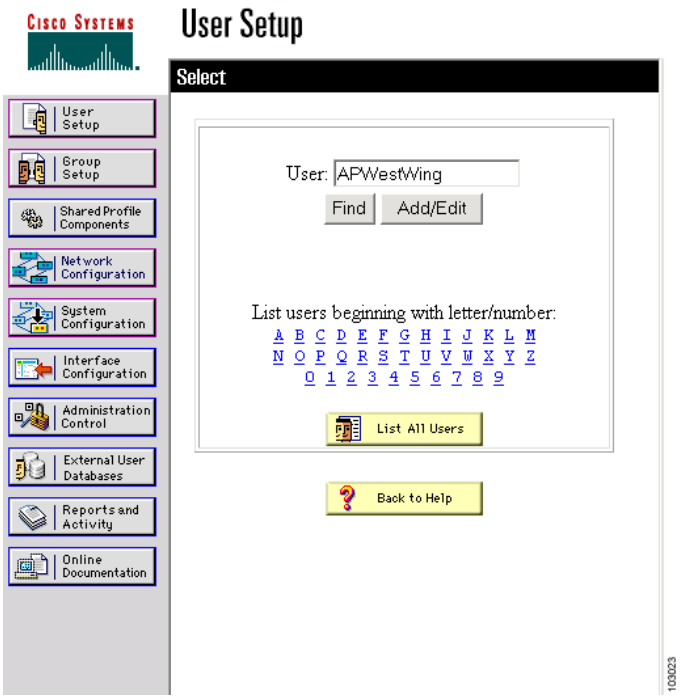
Step 6 From the Authenticate Using drop-down menu, select **RADIUS (Cisco Aironet)**.

Step 7 Click **Submit**.

Step 8 Repeat Step 2 through Step 7 for each WDS device candidate.

Step 9 Click **User Setup** to browse to the User Setup page. You must use the User Setup page to create entries for the access points that use the WDS device. Figure 11-12 shows the User Setup page.

Figure 11-12 User Setup Page

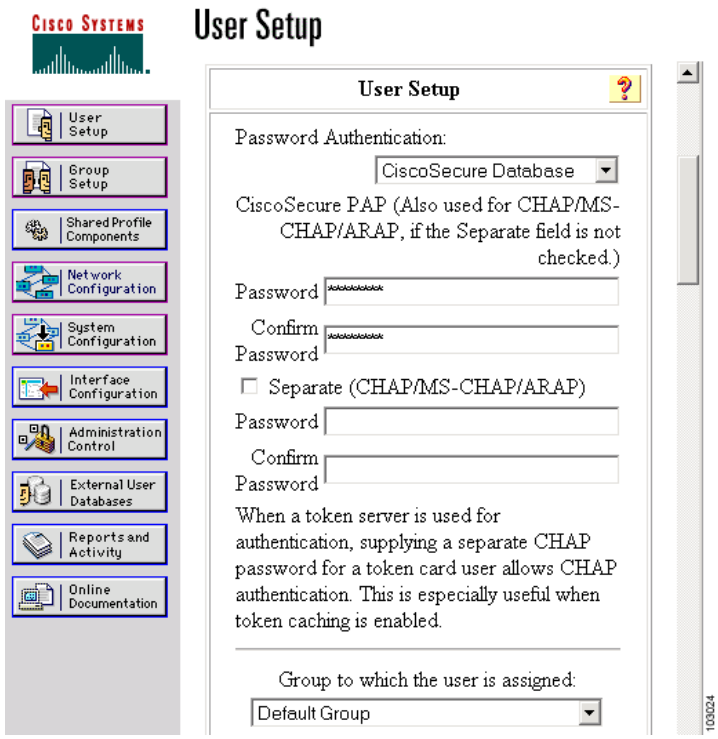


Step 10 Enter the name of the access point in the User field.

Step 11 Click **Add/Edit**.

Step 12 Scroll down to the User Setup box. Figure 11-13 shows the User Setup box.

Figure 11-13 ACS User Setup Box



Step 13 Select **CiscoSecure Database** from the Password Authentication drop-down menu.

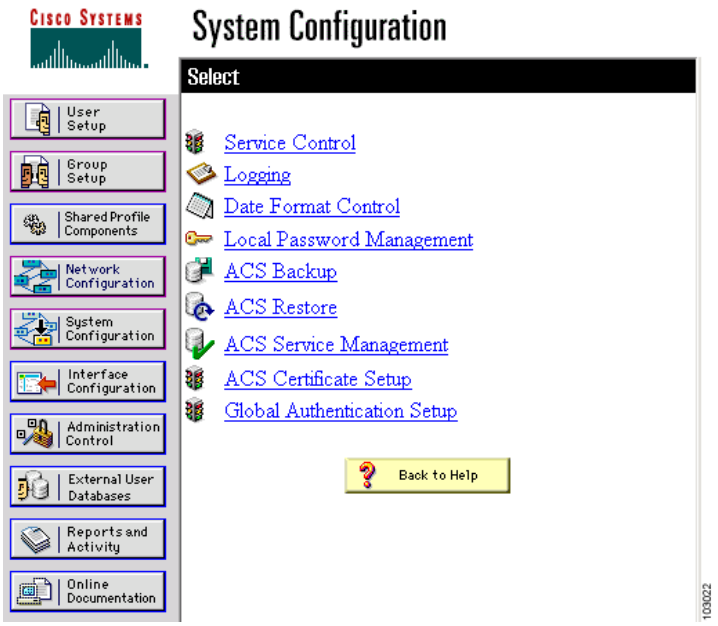
Step 14 In the Password and Confirm Password fields, enter exactly the same password that you entered on the access point on the Wireless Services AP page.

Step 15 Click **Submit**.

Step 16 Repeat Step 10 through Step 15 for each access point that uses the WDS device.

Step 17 Browse to the System Configuration page, click **Service Control**, and restart ACS to apply your entries. Figure 11-14 shows the System Configuration page.

Figure 11-14 ACS System Configuration Page



Viewing WDS Information

On the web-browser interface, browse to the Wireless Services Summary page to view a summary of WDS status.

On the CLI in privileged exec mode, use these commands to view information about the current WDS device and other access points participating in CCKM:

Command	Description
show wlccp ap	Use this command on access points participating in CCKM to display the WDS device's MAC address, the WDS device's IP address, the access point's state (authenticating, authenticated, or registered), the IP address of the infrastructure authenticator, and the IP address of the client device (MN) authenticator.
show wlccp wds { **ap** | **mn** } [**detail**] [**mac-addr** *mac-address*]	On the WDS device only, use this command to display cached information about access points and client devices. • **ap**—Use this option to display access points participating in CCKM. The command displays each access point's MAC address, IP address, state (authenticating, authenticated, or registered), and lifetime (seconds remaining before the access point must reauthenticate). Use the **mac-addr** option to display information about a specific access point. • **mn**—Use this option to display cached information about client devices, also called mobile nodes. The command displays each client's MAC address, IP address, the access point to which the client is associated (cur-AP), and state (authenticating, authenticated, or registered). Use the **detail** option to display the client's lifetime (seconds remaining before the client must reauthenticate), SSID, and VLAN ID. Use the **mac-addr** option to display information about a specific client device. If you only enter **show wlccp wds**, the command displays the access point's IP address, MAC address, priority, and interface state (administratively standalone, active, backup, or candidate). If the state is backup, the command also displays the current WDS device's IP address, MAC address, and priority.

Using Debug Messages

In privileged exec mode, use these debug commands to control the display of debug messages for devices interacting with the WDS device:

Command	Description
debug wlccp ap {**mn** | **wds-discovery** | **state**}	Use this command to turn on display of debug messages related to client devices (**mn**), the WDS discovery process, and access point authentication to the WDS device (**state**).
debug wlccp dump	Use this command to perform a dump of WLCCP packets received and sent in binary format.
debug wlccp packet	Use this command to turn on display of packets to and from the WDS device.
debug wlccp wds [**aggregator** | **authenticator** | **nm** | **state** | **statistics**]	Use this command and its options to turn on display of WDS debug messages. Use the **statistics** option to turn on display of failure statistics.
debug wlccp wds authenticator {**all** | **dispatcher** | **mac-authen** | **process** | **rxdata** | **state-machine** | **txdata**}	Use this command and its options to turn on display of WDS debug messages related to authentication.

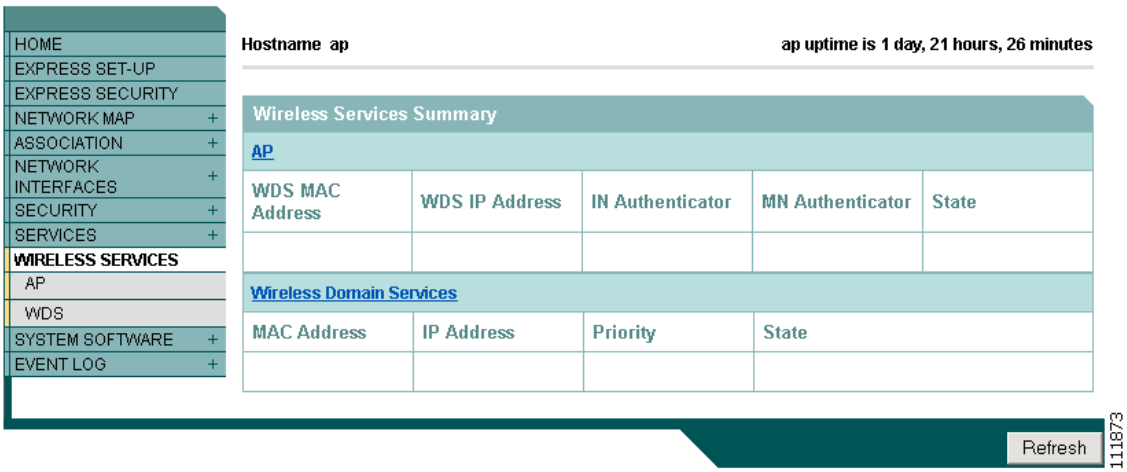
Configuring Radio Management

When you configure access points on your wireless LAN to use WDS, the access points automatically play a role in radio management when they interact with the WDS device. To complete the radio management configuration, you configure the WDS device to interact with the WLSE device on your network.

Follow these steps to enable radio management on an access point configured as a WDS device:

Step 1 Browse to the Wireless Services Summary page. Figure 11-15 shows the Wireless Services Summary page.

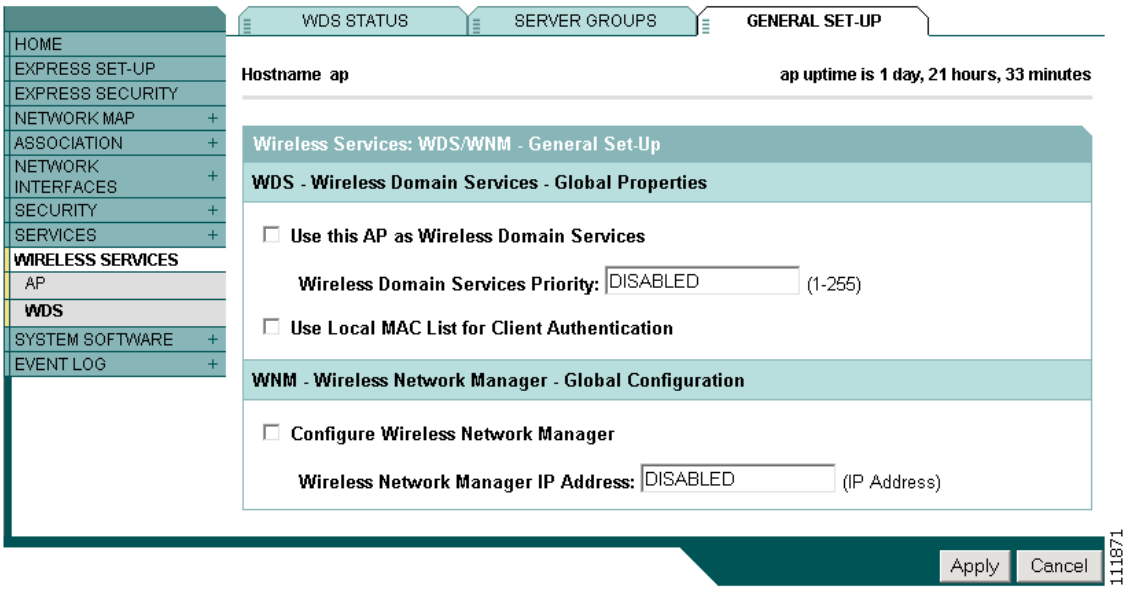
Figure 11-15 Wireless Services Summary Page



Step 2 Click **WDS** to browse to the General Setup page.

Step 3 On the WDS/WNM Summary page, click **Settings** to browse to the General Setup page. Figure 11-16 shows the General Setup page.

Figure 11-16 WDS/WNM General Setup Page



Step 4 Check the *Configure Wireless Network Manager* check box.

Step 5 In the *Wireless Network Manager IP Address* field, enter the IP address of the WLSE device on your network.

Step 6 Click **Apply**. The WDS access point is configured to interact with your WLSE device.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Radio Management" section on page 11-23:

```
AP# configure terminal
AP(config)# wlccp wnm ip address 192.250.0.5
AP(config)# end
```

In this example, the WDS access point is enabled to interact with a WLSE device with the IP address 192.250.0.5.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

CHAPTER 12

Configuring RADIUS and TACACS+ Servers

This chapter describes how to enable and configure the Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+), which provide detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS and TACACS+ are facilitated through AAA and can be enabled only through AAA commands.

Note You can configure your access point as a local authenticator to provide a backup for your main server or to provide authentication service on a network without a RADIUS server. See Chapter 8, "Configuring an Access Point as a Local Authenticator," for detailed instructions on configuring your access point as a local authenticator.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

This chapter contains these sections:

- Configuring and Enabling RADIUS, page 12-2
- Configuring and Enabling TACACS+, page 12-21

Configuring and Enabling RADIUS

This section describes how to configure and enable RADIUS. These sections describe RADIUS configuration:

- Understanding RADIUS, page 12-2
- RADIUS Operation, page 12-3
- Configuring RADIUS, page 12-4
- Displaying the RADIUS Configuration, page 12-17
- RADIUS Attributes Sent by the Access Point, page 12-18

Understanding RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, refer to the RADIUS server documentation.

Use RADIUS in these network environments, which require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that is customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as an access environment that uses a *smart card* access control system. In one case, RADIUS has been used with Enigma's security cards to validate users and to grant access to network resources.
- Networks already using RADIUS. You can add a Cisco access point containing a RADIUS client to the network.
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

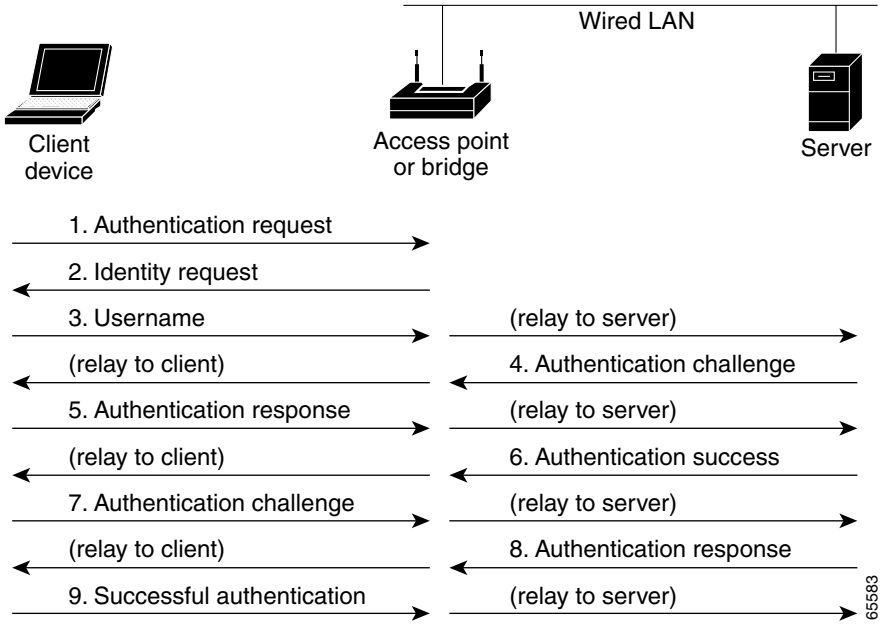
RADIUS is not suitable in these network security situations:

- Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.
- Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

RADIUS Operation

When a wireless user attempts to log in and authenticate to an access point whose access is controlled by a RADIUS server, authentication to the network occurs in the steps shown in Figure 12-1:

Figure 12-1 Sequence for EAP Authentication



In Steps 1 through 9 in Figure 12-1, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a WEP key that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the logon session.

During the logon session, the RADIUS server encrypts and sends the WEP key, called a *session key*, over the wired LAN to the access point. The access point encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the access point behaves the same way for each type: it relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the "Assigning Authentication Types to an SSID" section on page 10-10 for instructions on setting up client authentication using a RADIUS server.

Configuring RADIUS

This section describes how to configure your access point to support RADIUS. At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your access point.

This section contains this configuration information:

- Default RADIUS Configuration, page 12-4
- Identifying the RADIUS Server Host, page 12-4 (required)
- Configuring RADIUS Login Authentication, page 12-7 (required)
- Defining AAA Server Groups, page 12-9 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 12-11 (optional)
- Starting RADIUS Accounting, page 12-12 (optional)
- Selecting the CSID Format, page 12-13 (optional)
- Configuring Settings for All RADIUS Servers, page 12-13 (optional)
- Configuring the Access Point to Use Vendor-Specific RADIUS Attributes, page 12-14 (optional)
- Configuring the Access Point for Vendor-Proprietary RADIUS Server Communication, page 12-15 (optional)
- Configuring WISPr RADIUS Attributes, page 12-16 (optional)

Note The RADIUS server CLI commands are disabled until you enter the **aaa new-model** command.

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the access point through the CLI.

Identifying the RADIUS Server Host

Access point-to-RADIUS-server communication involves several components:

- Host name or IP address
- Authentication destination port
- Accounting destination port

- Key string
- Timeout period
- Retransmission value

You identify RADIUS security servers by their host name or IP address, host name and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service—such as accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the access point tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the access point use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the access point.

The timeout, retransmission, and encryption key values can be configured globally per server for all RADIUS servers or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the access point, use the three unique global configuration commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** global configuration command.

Note If you configure both global and per-server functions (timeout, retransmission, and key commands) on the access point, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these setting on all RADIUS servers, see the "Configuring Settings for All RADIUS Servers" section on page 12-13.

You can configure the access point to use AAA server groups to group existing server hosts for authentication. For more information, see the "Defining AAA Server Groups" section on page 12-9.

Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	Specify the IP address or host name of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command.

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
AP(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
AP(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

This example shows how to configure *host1* as the RADIUS server and to use the default ports for both authentication and accounting:

```
AP(config)# radius-server host host1
```

Note You also need to configure some settings on the RADIUS server. These settings include the IP address of the access point and the key string to be shared by both the server and the access point. For more information, refer to the RADIUS server documentation.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. For more information on list names, click this link: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **line**—Use the line password for authentication. You must define a line password before you can use this authentication method. Use the **password** *password* line configuration command. • **local**—Use the local username database for authentication. You must enter username information in the database. Use the **username** *password* global configuration command. • **radius**—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the "Identifying the RADIUS Server Host" section on page 12-4.
Step 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	**login authentication** {**default** | *list-name*}	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	**radius-server attribute 32 include-in-access-req format %h**	Configure the access point to send its system name in the NAS_ID attribute for authentication.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** {**default** \| *list-name*} line configuration command.

Defining AAA Server Groups

You can configure the access point to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	Specify the IP address or host name of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	**aaa group server radius** *group-name*	Define the AAA server-group with a group name. This command puts the access point in a server group configuration mode.
Step 5	**server** *ip-address*	Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.
Step 9		Enable RADIUS login authentication. See the "Configuring RADIUS Login Authentication" section on page 12-7.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server** *ip-address* server group configuration command.

In this example, the access point is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the access point uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

Note This section describes setting up authorization for access point adminsitrators, not for wireless client devices.

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa authorization network radius**	Configure the access point for user RADIUS authorization for all network-related service requests.
Step 3	**aaa authorization exec radius**	Configure the access point for user RADIUS authorization to determine if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Starting RADIUS Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the access point reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing. See the "RADIUS Attributes Sent by the Access Point" section on page 12-18 for a complete list of attributes sent and honored by the access point.

Beginning in privileged EXEC mode, follow these steps to enable RADIUS accounting for each Cisco IOS privilege level and for network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa accounting network start-stop radius**	Enable RADIUS accounting for all network-related service requests.
Step 3	**ip radius source-interface bvi1**	Configure the access point to send its BVI IP address in the NAS_IP_ADDRESS attribute for accounting records.
Step 4	**aaa accounting update periodic** *minutes*	Enter an accounting update interval in minutes.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable accounting, use the **no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* global configuration command.

Selecting the CSID Format

You can select the format for MAC addresses in Called-Station-ID (CSID) and Calling-Station-ID attributes in RADIUS packets. Use the **dot11 aaa csid** global configuration command to select the CSID format. Table 12-1 lists the format options with corresponding MAC address examples.

Table 12-1 CSID Format Options

Option	MAC Address Example
default	0007.85b3.5f4a
ietf	00-07-85-b3-5f-4a
unformatted	000785b35f4a

To return to the default CSID format, use the **no** form of the **dot11 aaa csid** command, or enter **dot11 aaa csid default**.

Note You can also use the **wlccp wds aaa csid** command to select the CSID format.

Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure global communication settings between the access point and all RADIUS servers:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server key** *string*	Specify the shared secret text string used between the access point and all RADIUS servers. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 3	**radius-server retransmit** *retries*	Specify the number of times the access point sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.
Step 4	**radius-server timeout** *seconds*	Specify the number of seconds an access point waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.
Step 5	**radius-server deadtime** *minutes*	Use this command to cause the Cisco IOS software to mark as “dead” any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to a maximum of 1440 (24 hours). **Note** If you set up more than one RADIUS server, you must configure the RADIUS server deadtime for optimal performance.

	Command	Purpose
Step 6	**radius-server attribute 32 include-in-access-req format %h**	Configure the access point to send its system name in the NAS_ID attribute for authentication.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your settings.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting for retransmit, timeout, and deadtime, use the **no** forms of these commands.

Configuring the Access Point to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the access point and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor ID is 9, and the supported option has vendor type 1, which is named *cisco-avpair*. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate AV pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and the asterisk (*) for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair activates Cisco's *multiple named ip address pools* feature during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= ″ip:addr-pool=first″
```

The following example shows how to provide a user logging in from an access point with immediate access to privileged EXEC commands:

```
cisco-avpair= ″shell:priv-lvl=15″
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, refer to RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

Beginning in privileged EXEC mode, follow these steps to configure the access point to recognize and use VSAs:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server vsa send** [**accounting** | **authentication**]	Enable the access point to recognize and use VSAs as defined by RADIUS IETF attribute 26. • (Optional) Use the **accounting** keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the **authentication** keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your settings.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

For a complete list of RADIUS attributes or more information about VSA 26, refer to the "RADIUS Attributes" appendix in the *Cisco IOS Security Configuration Guide for Release 12.2*.

Configuring the Access Point for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the access point and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the access point. You specify the RADIUS host and secret text string by using the **radius-server** global configuration commands.

Beginning in privileged EXEC mode, follow these steps to specify a vendor-proprietary RADIUS server host and a shared secret text string:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server host** {*hostname* | *ip-address*} **non-standard**	Specify the IP address or host name of the remote RADIUS server host and identify that it is using a vendor-proprietary implementation of RADIUS.

	Command	Purpose
Step 3	**radius-server key** *string*	Specify the shared secret text string used between the access point and the vendor-proprietary RADIUS server. The access point and the RADIUS server use this text string to encrypt passwords and exchange responses. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your settings.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete the vendor-proprietary RADIUS host, use the **no radius-server host** {*hostname* | *ip-address*} **non-standard** global configuration command. To disable the key, use the **no radius-server key** global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of *rad124* between the access point and the server:

```
AP(config)# radius-server host 172.20.30.15 nonstandard
AP(config)# radius-server key rad124
```

Configuring WISPr RADIUS Attributes

The Wi-Fi Alliance's *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document lists RADIUS attributes that access points must send with RADIUS accounting and authentication requests. The access point currently supports only the WISPr location-name and the ISO and International Telecommunications Union (ITU) country and area codes attributes. Use the **snmp-server location** and the **dot11 location isocc** commands to configure these attributes on the access point.

The *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document also requires the access point to include a class attribute in RADIUS authentication replies and accounting requests. The access point includes the class attribute automatically and does not have to be configured to do so.

You can find a list of ISO and ITU country and area codes at the ISO and ITU websites. Cisco IOS software does not check the validity of the country and area codes that you configure on the access point.

Beginning in privileged EXEC mode, follow these steps to specify WISPr RADIUS attributes on the access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server location** *location*	Specify the WISPr location-name attribute. The *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document recommends that you enter the location name in this format: *hotspot_operator_name*,*location*
Step 3	**dot11 location isocc** *ISO-country-code* **cc** *country-code* **ac** *area-code*	Specify ISO and ITU country and area codes that the access point includes in accounting and authentication requests. • **isocc** *ISO-country-code*—specifies the ISO country code that the access point includes in RADIUS authentication and accounting requests • **cc** *country-code*—specifies the ITU country code that the access point includes in RADIUS authentication and accounting requests • **ac** *area-code*—specifies the ITU area code that the access point includes in RADIUS authentication and accounting requests
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your settings.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure the WISPr location-name attribute:

```
ap# snmp-server location ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
```

This example shows how to configure the ISO and ITU location codes on the access point:

```
ap# dot11 location isocc us cc 1 ac 408
```

This example shows how the access point adds the SSID used by the client device and formats the location-ID string:

```
isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport
```

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** privileged EXEC command.

Note When DNS is configured on the access point, the **show running-config** command sometimes displays a server's IP address instead of its name.

RADIUS Attributes Sent by the Access Point

Table 12-2 through Table 12-6 identify the attributes sent by an access point to a client in access-request, access-accept, and accounting-request packets.

Note You can configure the access point to include in its RADIUS accounting and authentication requests attributes recommeded by the Wi-Fi Alliance's *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document. Refer to the "Configuring WISPr RADIUS Attributes" section on page 12-16 for instructions.

Table 12-2 Attributes Sent in Access-Request Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
12	Framed-MTU
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier[1]
61	NAS-Port-Type
79	EAP-Message
80	Message-Authenticator

1. The access point sends the NAS-Identifier if attribute 32 (include-in-access-req) is configured.

Table 12-3 Attributes Honored in Access-Accept Packets

Attribute ID	Description
25	Class
27	Session-Timeout
64	Tunnel-Type[1]
65	Tunnel-Medium-Type[1]
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID[1]
VSA (attribute 26)	LEAP session-key
VSA (attribute 26)	Auth-Algo-Type
VSA (attribute 26)	SSID

1. RFC2868; defines a VLAN override number.

Table 12-4 Attributes Sent in Accounting-Request (start) Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
44	Acct-Session-Id
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface

Table 12-5 Attributes Sent in Accounting-Request (update) Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	VLAN-ID
VSA (attribute 26)	Connect-Progress
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface

Table 12-6 Attributes Sent in Accounting-Request (stop) Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	Disc-Cause-Ext
VSA (attribute 26)	VLAN-ID
VSA (attribute 26)	Connect-Progress
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface
VSA (attribute 26)	Auth-Algo-Type

Note By default, the access point sends reauthentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers do not support the authenticate-only service-type attribute. Changing the service-type attribute to login-only ensures that Microsoft IAS servers recognize reauthentication requests from the access point. Use the **dot11 aaa authentication attributes service-type login-only** global configuration command to set the service-type attribute in reauthentication requests to login-only.

Configuring and Enabling TACACS+

This section contains this configuration information:

- Understanding TACACS+, page 12-21
- TACACS+ Operation, page 12-22
- Configuring TACACS+, page 12-22
- Displaying the TACACS+ Configuration, page 12-27

Understanding TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your access point. Unlike RADIUS, TACACS+ does not authenticate client devices associated to the access point.

TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You should have access to and should configure a TACACS+ server before configuring TACACS+ features on your access point.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

TACACS+, administered through the AAA security services, can provide these services:

- Authentication—Provides complete control of authentication of administrators through login and password dialog, challenge and response, and messaging support.

  The authentication facility can conduct a dialog with the administrator (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother's maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to administrator screens. For example, a message could notify administrators that their passwords must be changed because of the company's password aging policy.

- Authorization—Provides fine-grained control over administrator capabilities for the duration of the administrator's session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on the commands that an administrator can execute with the TACACS+ authorization feature.

- Accounting—Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track administrator activity for a security audit or to provide information for user billing. Accounting records include administrator identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the access point and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the access point and the TACACS+ daemon are encrypted.

You need a system running the TACACS+ daemon software to use TACACS+ on your access point.

TACACS+ Operation

When an administrator attempts a simple ASCII login by authenticating to an access point using TACACS+, this process occurs:

1. When the connection is established, the access point contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the administrator. The administrator enters a username, and the access point then contacts the TACACS+ daemon to obtain a password prompt. The access point displays the password prompt to the administrator, the administrator enters a password, and the password is then sent to the TACACS+ daemon.

   TACACS+ allows a conversation to be held between the daemon and the administrator until the daemon receives enough information to authenticate the administrator. The daemon prompts for a username and password combination, but can include other items, such as the user's mother's maiden name.

2. The access point eventually receives one of these responses from the TACACS+ daemon:
   - ACCEPT—The administrator is authenticated and service can begin. If the access point is configured to require authorization, authorization begins at this time.
   - REJECT—The administrator is not authenticated. The administrator can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
   - ERROR—An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the access point. If an ERROR response is received, the access point typically tries to use an alternative method for authenticating the administrator.
   - CONTINUE—The administrator is prompted for additional authentication information.

   After authentication, the administrator undergoes an additional authorization phase if authorization has been enabled on the access point. Administrators must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that administrator, determining the services that the administrator can access:
   - Telnet, rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and administrator timeouts

Configuring TACACS+

This section describes how to configure your access point to support TACACS+. At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting. A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on an administrator. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on administrators; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

This section contains this configuration information:

- Default TACACS+ Configuration, page 12-23
- Identifying the TACACS+ Server Host and Setting the Authentication Key, page 12-23
- Configuring TACACS+ Login Authentication, page 12-24
- Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 12-25
- Starting TACACS+ Accounting, page 12-26

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate administrators accessing the access point through the CLI.

Identifying the TACACS+ Server Host and Setting the Authentication Key

You can configure the access point to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	Identify the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them. • For *hostname*, specify the name or IP address of the host. • (Optional) For **port** *integer*, specify a server port number. The default is port 49. The range is 1 to 65535. • (Optional) For **timeout** *integer*, specify a time in seconds the access point waits for a response from the daemon before it times out and declares an error. The default is 5 seconds. The range is 1 to 1000 seconds. • (Optional) For **key** *string*, specify the encryption key for encrypting and decrypting all traffic between the access point and the TACACS+ daemon. You must configure the same key on the TACACS+ daemon for encryption to be successful.
Step 3	**aaa new-model**	Enable AAA.
Step 4	**aaa group server tacacs+** *group-name*	(Optional) Define the AAA server-group with a group name. This command puts the access point in a server group subconfiguration mode.

	Command	Purpose
Step 5	**server** *ip-address*	(Optional) Associate a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show tacacs**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the specified TACACS+ server name or address, use the **no tacacs-server host** *hostname* global configuration command. To remove a server group from the configuration list, use the **no aaa group server tacacs+** *group-name* global configuration command. To remove the IP address of a TACACS+ server, use the **no server ip-address** server group subconfiguration command.

Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate an administrator. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the administrator access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **line**—Use the line password for authentication. You must define a line password before you can use this authentication method. Use the **password** *password* line configuration command. • **local**—Use the local username database for authentication. You must enter username information into the database. Use the **username** *password* global configuration command. • **tacacs+**—Uses TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.
Step 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	**login authentication** {**default** | *list-name*}	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] global configuration command. To either disable TACACS+ authentication for logins or to return to the default value, use the **no login authentication** {**default** \| *list-name*} line configuration command.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to an administrator. When AAA authorization is enabled, the access point uses information retrieved from the administrator's profile, which is located either in the local user database or on the security server, to configure the administrator's session. The administrator is granted access to a requested service only if the information in the administrator profile allows it.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict an administrator's network access to privileged EXEC mode.

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

Note Authorization is bypassed for authenticated administrators who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa authorization network tacacs+**	Configure the access point for administrator TACACS+ authorization for all network-related service requests.
Step 3	**aaa authorization exec tacacs+**	Configure the access point for administrator TACACS+ authorization to determine if the administrator has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Starting TACACS+ Accounting

The AAA accounting feature tracks the services that administrators are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the access point reports administrator activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting for each Cisco IOS privilege level and for network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa accounting network start-stop tacacs+**	Enable TACACS+ accounting for all network-related service requests.
Step 3	**aaa accounting exec start-stop tacacs+**	Enable TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.
Step 4	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable accounting, use the **no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* global configuration command.

Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the **show tacacs** privileged EXEC command.

CHAPTER 13

Configuring VLANs

This chapter describes how to configure your access point to operate with the VLANs set up on your wired LAN. These sections describe how to configure your access point to support VLANs:

- Understanding VLANs, page 13-2
- Configuring VLANs, page 13-4
- VLAN Configuration Example, page 13-7

Understanding VLANs

A VLAN is a switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

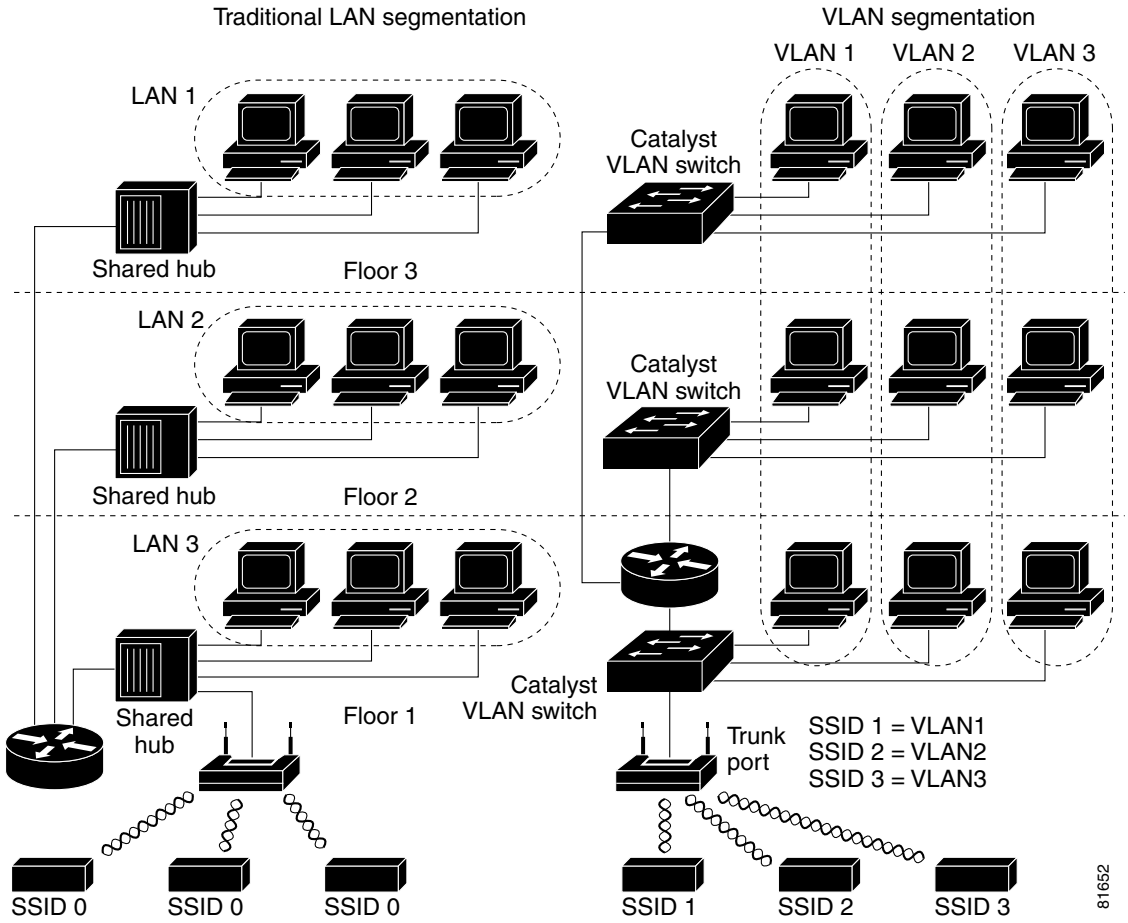
VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. You should consider several key issues when designing and building switched LAN networks:

- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

You extend VLANs into a wireless LAN by adding IEEE 802.11Q tag awareness to the access point. Frames destined for different VLANs are transmitted by the access point wirelessly on different SSIDs with different WEP keys. Only the clients associated with that VLAN receive those packets. Conversely, packets coming from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded onto the wired network.

Figure 13-1 shows the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 13-1 LAN and VLAN Segmentation with Wireless Devices



Related Documents

These documents provide more detailed information pertaining to VLAN design and configuration:

- *Cisco IOS Switching Services Configuration Guide.* Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/index.htm
- *Cisco Internetwork Design Guide.* Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/index.htm
- *Cisco Internetworking Technology Handbook.* Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm
- *Cisco Internetworking Troubleshooting Guide.* Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm

Incorporating Wireless Devices into VLANs

The basic wireless components of a VLAN consist of an access point and a client associated to it using wireless technology. The access point is physically connected through a trunk port to the network VLAN switch on which the VLAN is configured. The physical connection to the VLAN switch is through the access point's Ethernet port.

In fundamental terms, the key to configuring an access point to connect to a specific VLAN is by configuring its SSID to recognize that VLAN. Since VLANs are identified by a VLAN ID, it follows that if the SSID on an access point is configured to recognize a specific VLAN ID, a connection to the VLAN is established. When this connection is made, associated wireless client devices having the same SSID can access the VLAN through the access point. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections. You can configure up to 16 SSIDs on your access point, so you can support up to 16 VLANs. You can assign only one SSID to a VLAN.

You can use the VLAN feature to deploy wireless devices with greater efficiency and flexibility. For example, one access point can now handle the specific requirements of multiple users having widely varied network access and permissions. Without VLAN capability, multiple access points would have to be employed to serve classes of users based on the access and permissions they were assigned.

These are two common strategies for deploying wireless VLANs:

- Segmentation by user groups: You can segment your wireless LAN user community and enforce a different security policy for each user group. For example, you can create three wired and wireless VLANs in an enterprise environment for full-time and part-time employees and also provide guest access.
- Segmentation by device types: You can segment your wireless LAN to allow different devices with different security capabilities to join the network. For example, some wireless users might have handheld devices that support only static WEP, and some wireless users might have more sophisticated devices using dynamic WEP. You can group and isolate these devices into separate VLANs.

Note You cannot configure multiple VLANs on repeater access points. Repeater access points support only the native VLAN.

Configuring VLANs

These sections describe how to configure VLANs on your access point:

- Configuring a VLAN, page 13-4
- Using a RADIUS Server to Assign Users to VLANs, page 13-6
- Viewing VLANs Configured on the Access Point, page 13-6

Configuring a VLAN

Configuring your access point to support VLANs is a three-step process:

1. Enable the VLAN on the radio and Ethernet ports.
2. Assign SSIDs to VLANs.
3. Assign authentication settings to SSIDs.

This section describes how to assign SSIDs to VLANs and how to enable a VLAN on the access point radio and Ethernet ports. For detailed instructions on assigning authentication types to SSIDs, see Chapter 10, "Configuring Authentication Types." For instructions on assigning other settings to SSIDs, see Chapter 7, "Configuring Multiple SSIDs."

You can configure up to 16 SSIDs on the access point, so you can support up to 16 VLANs that are configured on your LAN.

Beginning in privileged EXEC mode, follow these steps to assign an SSID to a VLAN and enable the VLAN on the access point radio and Ethernet ports:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio0**	Enter interface configuration mode for the radio interface.
Step 3	**ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. **Note** You use the **ssid** command's authentication options to configure an authentication type for each SSID. See Chapter 10, "Configuring Authentication Types," for instructions on configuring authentication types.
Step 4	**vlan** *vlan-id*	(Optional) Assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. Enter a VLAN ID from 1 to 4095. You can assign only one SSID to a VLAN.
Step 5	**exit**	Return to interface configuration mode for the radio interface.
Step 6	**interface dot11radio0.x**	Enter interface configuration mode for the radio VLAN sub interface.
Step 7	**encapsulation dot1q** *vlan-id* [**native**]	Enable a VLAN on the radio interface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.
Step 8	**exit**	Return to global configuration mode.
Step 9	**interface fastEthernet0.x**	Enter interface configuration mode for the Ethernet VLAN subinterface.
Step 10	**encapsulation dot1q** *vlan-id* [**native**]	Enable a VLAN on the Ethernet interface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to:

- Name an SSID
- Assign the SSID to a VLAN
- Enable the VLAN on the radio and Ethernet ports as the native VLAN

```
ap1200# configure terminal
ap1200(config)# interface dot11radio0
```

```
ap1200(config-if)# ssid batman
ap1200(config-ssid)# vlan 1
ap1200(config-ssid)# exit
ap1200(config)# interface dot11radio0.1
ap1200(config-subif)# encapsulation dot1q 1 native
ap1200(config-subif)# exit
ap1200(config)# interface fastEthernet0.1
ap1200(config-subif)# encapsulation dot1q 1 native
ap1200(config-subif)# exit
ap1200(config)# end
```

Using a RADIUS Server to Assign Users to VLANs

You can configure your RADIUS authentication server to assign users or groups of users to a specific VLAN when they authenticate to the network.

Note Unicast and multicast cipher suites advertised in WPA information element (and negotiated during 802.11 association) may potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new vlan ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the access point and client to switch back to the new cipher suite. Currently, the WPA and CCKM protocols do not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the client device is disassociated from the wireless LAN.

The VLAN-mapping process consists of these steps:

1. A client device associates to the access point using any SSID configured on the access point.
2. The client begins RADIUS authentication.
3. When the client authenticates sucessfully, the RADIUS server maps the client to a specific VLAN, regardless of the VLAN mapping defined for the SSID the client is using on the access point. If the server does not return any VLAN attribute for the client, the client is assigned to the VLAN specified by the SSID mapped locally on the access point.

These are the RADIUS user attributes used for vlan-id assignment. Each attribute must have a common tag value between 1 and 31 to identify the grouped relationship.

- IETF 64 (Tunnel Type): Set this attribute to **VLAN**
- IETF 65 (Tunnel Medium Type): Set this attribute to **802**
- IETF 81 (Tunnel Private Group ID): Set this attribute to *vlan-id*

Viewing VLANs Configured on the Access Point

In privileged EXEC mode, use the **show vlan** command to view the VLANs that the access point supports. This is sample output from a **show vlan** command:

```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

 This is configured as native Vlan for the following interface(s) :
```

```
Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 1             201688                  0
        Bridging        Bridge Group 1             201688                  0
        Bridging        Bridge Group 1             201688                  0

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.2
FastEthernet0.2
Virtual-Dot11Radio0.2

   Protocols Configured:   Address:              Received:        Transmitted:
```

VLAN Configuration Example

This example shows how to use VLANs to manage wireless devices on a college campus. In this example, three levels of access are available through VLANs configured on the wired network:

- Management access—Highest level of access; users can access all internal drives and files, departmental databases, top-level financial information, and other sensitive information. Management users are required to authenticate using Cisco LEAP.
- Faculty access—Medium level of access; users can access school's Intranet and Internet, access internal files, access student databases, and view internal information such as human resources, payroll, and other faculty-related material. Faculty users are required to authenticate using Cisco LEAP.
- Student access—Lowest level of access; users can access school's Intranet and the Internet, obtain class schedules, view grades, make appointments, and perform other student-related activities. Students are allowed to join the network using static WEP.

In this scenario, a minimum of three VLAN connections are required, one for each level of access. Because the access point can handle up to 16 SSIDs, you can use the basic design shown in Table 13-1.

Table 13-1 Access Level SSID and VLAN Assignment

Level of Access	SSID	VLAN ID
Management	boss	01
Faculty	teach	02
Student	learn	03

Managers configure their wireless client adapters to use SSID boss, faculty members configure their clients to use SSID teach, and students configure their wireless client adapters to use SSID learn. When these clients associate to the access point, they automatically belong to the correct VLAN.

You would complete these steps to support the VLANs in this example:

1. Configure or confirm the configuration of these VLANs on one of the switches on your LAN.
2. On the access point, assign an SSID to each VLAN.
3. Assign authentication types to each SSID.

4. Configure VLAN 1, the Management VLAN, on both the fastethernet and dot11radio interfaces on the access point. You should make this VLAN the native VLAN.
5. Configure VLANs 2 and 3 on both the fastethernet and dot11radio interfaces on the access point.
6. Configure the client devices.

Table 13-2 shows the commands needed to configure the three VLANs in this example.

Table 13-2 Configuration Commands for VLAN Example

Configuring VLAN 1	Configuring VLAN 2	Configuring VLAN 3
ap1200# **configure terminal** ap1200(config)# **interface dot11radio 0** ap1200(config-if)# **ssid boss** ap1200(config-ssid)# **vlan 01** ap1200(config-ssid)# **end**	ap1200# **configure terminal** ap1200(config)# **interface dot11radio 0** ap1200(config-if)# **ssid teach** ap1200(config-ssid)# **vlan 02** ap1200(config-ssid)# **end**	ap1200# **configure terminal** ap1200(config)# **interface dot11radio 0** ap1200(config-if)# **ssid learn** ap1200(config-ssid)# **vlan 03** ap1200(config-ssid)# **end**
ap1200 **configure terminal** ap1200(config) **interface FastEthernet0.1** ap1200(config-subif) **encapsulation dot1Q 1 native** ap1200(config-subif) **exit**	ap1200(config) **interface FastEthernet0.2** ap1200(config-subif) **encapsulation dot1Q 2** ap1200(config-subif) **bridge-group 2** ap1200(config-subif) **exit**	ap1200(config) **interface FastEthernet0.3** ap1200(config-subif) **encapsulation dot1Q 3** ap1200(config-subif) **bridge-group 3** ap1200(config-subif) **exit**
ap1200(config)# **interface Dot11Radio0.1** ap1200(config-subif)# **encapsulation dot1Q 1 native** ap1200(config-subif)# **exit** **Note** You do not need to configure a bridge group on the subinterface that you set up as the native VLAN. This bridge group is moved to the native subinterface automatically to maintain the link to BVI 1, which represents both the radio and Ethernet interfaces.	ap1200(config) **interface Dot11Radio0.2** ap1200(config-subif) **encapsulation dot1Q 2** ap1200(config-subif) **bridge-group 2** ap1200(config-subif) **exit**	ap1200(config) **interface Dot11Radio0.3** ap1200(config-subif) **encapsulation dot1Q 3** ap1200(config-subif) **bridge-group 3** ap1200(config-subif) **exit**

Table 13-3 shows the results of the configuration commands in Table 13-2. Use the **show running** command to display the running configuration on the access point.

Table 13-3 Results of Example Configuration Commands

VLAN 1 Interfaces	VLAN 2 Interfaces	VLAN 3 Interfaces
interface Dot11Radio0.1 encapsulation dot1Q 1 native no ip route-cache no cdp enable bridge-group 1 bridge-group 1 subscriber-loop-control bridge-group 1 block-unknown-source no bridge-group 1 source-learning no bridge-group 1 unicast-flooding bridge-group 1 spanning-disabled	interface Dot11Radio0.2 encapsulation dot1Q 2 no ip route-cache no cdp enable bridge-group 2 bridge-group 2 subscriber-loop-control bridge-group 2 block-unknown-source no bridge-group 2 source-learning no bridge-group 2 unicast-flooding bridge-group 2 spanning-disabled	interface Dot11Radio0.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 bridge-group 3 subscriber-loop-control bridge-group 3 block-unknown-source no bridge-group 3 source-learning no bridge-group 3 unicast-flooding bridge-group 3 spanning-disabled
interface FastEthernet0.1 encapsulation dot1Q 1 native no ip route-cache bridge-group 1 no bridge-group 1 source-learning bridge-group 1 spanning-disabled	interface FastEthernet0.2 encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled	interface FastEthernet0.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 no bridge-group 3 source-learning bridge-group 3 spanning-disabled

Notice that when you configure a bridge group on the radio interface, these commands are set automatically:

```
bridge-group 2 subscriber-loop-control
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
bridge-group 2 spanning-disabled
```

When you configure a bridge group on the FastEthernet interface, these commands are set automatically:

```
no bridge-group 2 source-learning
bridge-group 2 spanning-disabled
```

CHAPTER 14

Configuring QoS

This chapter describes how to configure quality of service (QoS) on your access point. With this feature, you can provide preferential treatment to certain traffic at the expense of others. Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release.

This chapter consists of these sections:

- Understanding QoS for Wireless LANs, page 14-2
- Configuring QoS, page 14-4
- QoS Configuration Examples, page 14-10

Understanding QoS for Wireless LANs

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure QoS on the access point, you can select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your wireless LAN makes network performance more predictable and bandwidth utilization more effective.

When you configure QoS, you create QoS policies and apply the policies to the VLANs configured on your access point. If you do not use VLANs on your network, you can apply your QoS policies to the access point's Ethernet and radio ports.

QoS for Wireless LANs Versus QoS on Wired LANs

The QoS implementation for wireless LANs differs from QoS implementations on other Cisco devices. With QoS enabled, access points perform the following:

- They do not classify packets; they prioritize packets based on DSCP value, client type (such as a wireless phone), or the priority value in the 802.1q or 802.1p tag.
- They do not construct internal DSCP values; they only support mapping by assigning IP DSCP, Precedence, or Protocol values to Layer 2 CoS values. Table 14-1 lists the CoS values as they map to DSCP values.

Table 14-1 CoS Values Mapped to DSCP Values

CoS Value	DSCP Value
1	10
2	18
3	26
4	34
5	46
6	48
7	56

- They carry out EDCF like queuing on the radio egress port only.
- They do only FIFO queueing on the Ethernet egress port.
- They support only 802.1Q/P tagged packets. Access points do not support ISL.
- They support only MQC policy-map **set cos** action.
- They prioritize the traffic from voice clients (such as Symbol phones) over traffic from other clients when the QoS Element for Wireless Phones feature is enabled.
- They support Spectralink phones using the class-map IP protocol clause with the protocol value set to 119.

To contrast the wireless LAN QoS implementation with the QoS implementation on other Cisco network devices, see the *Cisco IOS Quality of Service Solutions Configuration Guide* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm

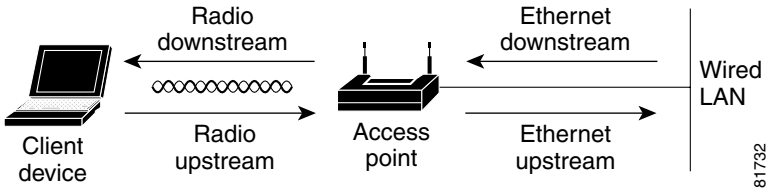
Impact of QoS on a Wireless LAN

Wireless LAN QoS features are a subset of the proposed 802.11e draft. QoS on wireless LANs provides prioritization of traffic from the access point over the WLAN based on traffic classification.

Just as in other media, you might not notice the effects of QoS on a lightly loaded wireless LAN. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.

QoS on the wireless LAN focuses on downstream prioritization from the access point. Figure 14-1 shows the upstream and downstream traffic flow.

Figure 14-1 Upstream and Downstream Traffic Flow



- The radio downstream flow is traffic transmitted out the access point radio to a wireless client device. This traffic is the main focus for QoS on a wireless LAN.
- The radio upstream flow is traffic transmitted out the wireless client device to the access point. QoS for wireless LANs does not affect this traffic.
- The Ethernet downstream flow is traffic sent from a switch or a router to the Ethernet port on the access point. If QoS is enabled on the switch or router, the switch or router might prioritize and rate-limit traffic to the access point.
- The Ethernet upstream flow is traffic sent from the access point Ethernet port to a switch or router on the wired LAN. The access point does not prioritize traffic that it sends to the wired LAN based on traffic classification.

Precedence of QoS Settings

When you enable QoS, the access point queues packets based on the Layer 2 class of service value for each packet. The access point applies QoS policies in this order:

1. Packets already classified—When the access point receives packets from a QoS-enabled switch or router that has already classified the packets with non-zero 802.1Q/P user_priority values, the access point uses that classification and does not apply other QoS policy rules to the packets. An existing classification takes precedence over all other policies on the access point.

Note Even if you have not configured a QoS policy, the access point always honors tagged 802.1P packets that it receives over the radio interface.

2. *QoS Element for Wireless Phones* setting—If you enable the *QoS Element for Wireless Phones* setting, traffic from voice clients takes priority over other traffic regardless of other policy settings. The *QoS Element for Wireless Phones* setting takes precedence over other policies, second only to previously assigned packet classifications.
3. Policies you create on the access point—QoS Policies that you create and apply to VLANs or to the access point interfaces are third in precedence after previously classified packets and the *QoS Element for Wireless Phones* setting.
4. Default classification for all packets on VLAN—If you set a default classification for all packets on a VLAN, that policy is fourth in the precedence list.

Configuring QoS

QoS is disabled by default (however, the radio interface always honors tagged 802.1P packets even when you have not configured a QoS policy). This section describes how to configure QoS on your access point. It contains this configuration information:

- Configuration Guidelines, page 14-4
- Configuring QoS Using the Web-Browser Interface, page 14-4
- Adjusting Radio Access Categories, page 14-8
- Disabling AVVID Priority Mapping, page 14-10

Configuration Guidelines

Before configuring QoS on your access point, you should be aware of this information:

- The most important guideline in QoS deployment is to be familiar with the traffic on your wireless LAN. If you know the applications used by wireless client devices, the applications' sensitivity to delay, and the amount of traffic associated with the applications, you can configure QoS to improve performance.
- QoS does not create additional bandwidth for your wireless LAN; it helps control the allocation of bandwidth. If you have plenty of bandwidth on your wireless LAN, you might not need to configure QoS.

Configuring QoS Using the Web-Browser Interface

This section describes configuring QoS using the web-browser interface.

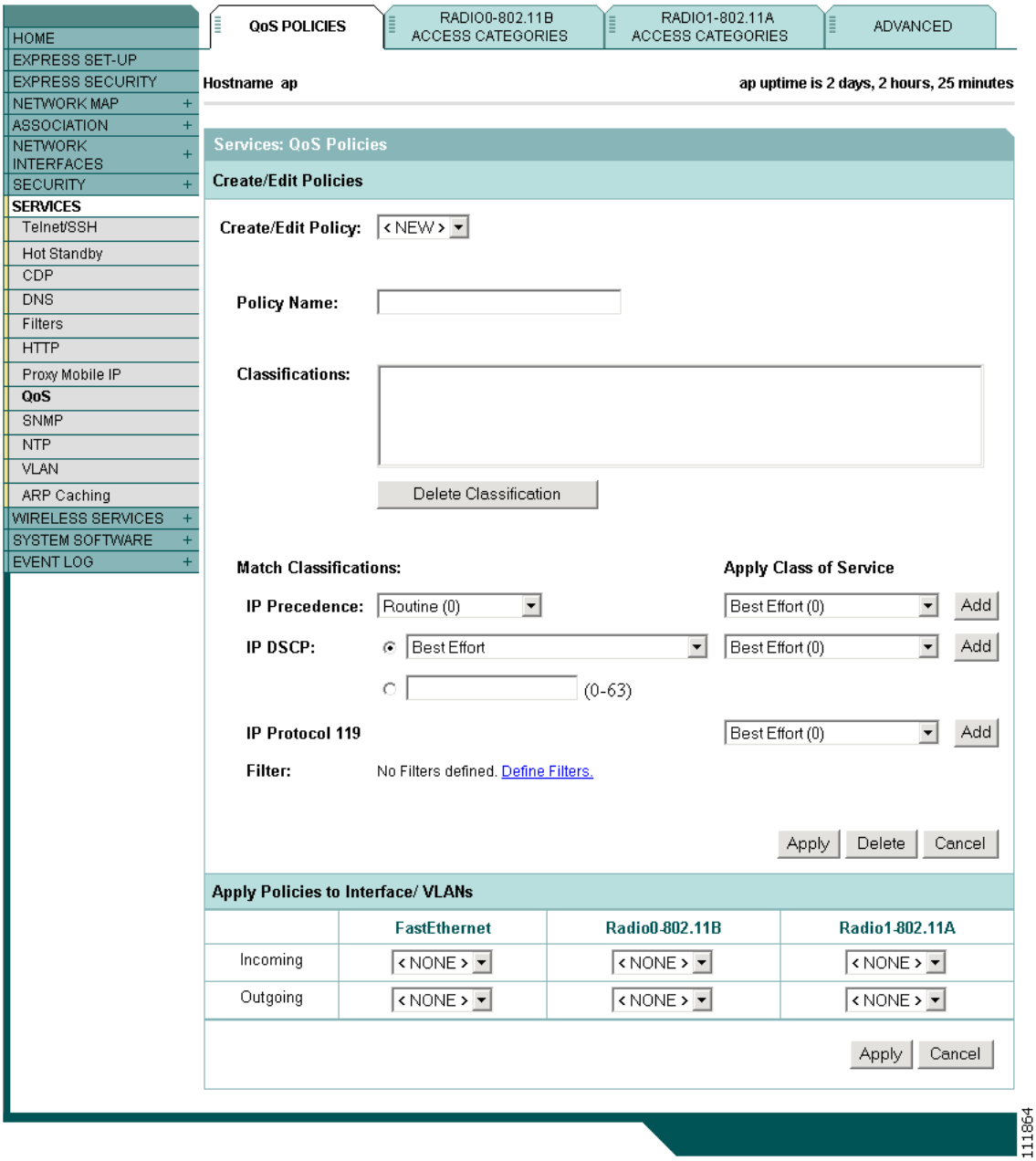
For a list of Cisco IOS commands for configuring QoS using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Follow these steps to configure QoS:

Step 1 If you use VLANs on your wireless LAN, make sure the necessary VLANs are configured on your access point before configuring QoS.

Step 2 Click **Services** in the task menu on the left side of any page in the web-browser interface. When the list of Services expands, click **QoS**. The QoS Policies page appears. Figure 14-2 shows the QoS Policies page.

Figure 14-2 QoS Policies Page



Step 3 With **<NEW>** selected in the Create/Edit Policy field, type a name for the QoS policy in the Policy Name entry field. The name can contain up to 25 alphanumeric characters. Do not include spaces in the policy name.

Step 4 If the packets that you need to prioritize contain IP precedence information in the IP header TOS field, select an IP precedence classification from the IP Precedence drop-down menu. Menu selections include:

- Routine (0)
- Priority (1)
- Immediate (2)
- Flash (3)
- Flash Override (4)
- Critic/CCP (5)
- Internet Control (6)
- Network Control (7)

Step 5 Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets of the type that you selected from the IP Precedence menu. The access point matches your IP Precedence selection with your class of service selection. Settings in the Apply Class of Service menu include:

- Best Effort (0)
- Background (1)
- Spare (2)
- Excellent (3)
- Control Lead (4)
- Video <100ms Latency (5)
- Voice <100ms Latency (6)
- Network Control (7)

Step 6 Click the **Add** button beside the Class of Service menu for IP Precedence. The classification appears in the Classifications field. To delete a classification, select it and click the **Delete** button beside the Classifications field.

Step 7 If the packets that you need to prioritize contain IP DSCP precedence information in the IP header TOS field, select an IP DSCP classification from the IP DSCP drop-down menu. Menu selections include:

- Best Effort
- Assured Forwarding — Class 1 Low
- Assured Forwarding — Class 1 Medium
- Assured Forwarding — Class 1 High
- Assured Forwarding — Class 2 Low
- Assured Forwarding — Class 2 Medium
- Assured Forwarding — Class 2 High
- Assured Forwarding — Class 3 Low
- Assured Forwarding — Class 3 Medium
- Assured Forwarding — Class 3 High
- Assured Forwarding — Class 4 Low
- Assured Forwarding — Class 4 Medium
- Assured Forwarding — Class 4 High

- Class Selector 1
- Class Selector 2
- Class Selector 3
- Class Selector 4
- Class Selector 5
- Class Selector 6
- Class Selector 7
- Expedited Forwarding

Step 8 Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets of the type that you selected from the IP DSCP menu. The access point matches your IP DSCP selection with your class of service selection.

Step 9 Click the **Add** button beside the Class of Service menu for IP DSCP. The classification appears in the Classifications field.

Step 10 If you need to prioritize the packets from Spectralink phones (IP Protocol 119) on your wireless LAN, use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to Spectralink phone packets. The access point matches Spectralink phone packets with your class of service selection.

Step 11 Click the **Add** button beside the Class of Service menu for IP Protocol 119. The classification appears in the Classifications field.

Step 12 If you need to assign a priority to filtered packets, use the Filter drop-down menu to select a Filter to include in the policy. (If no filters are defined on the access point, a link to the Apply Filters page appears instead of the Filter drop-down menu.) For example, you could assign a high priority to a MAC address filter that includes the MAC addresses of IP phones.

Note The access list you use in QoS does not affect the access point's packet forwarding decisions.

Step 13 Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets that match the filter that you selected from the Filter menu. The access point matches your filter selection with your class of service selection.

Step 14 Click the **Add** button beside the Class of Service menu for Filter. The classification appears in the Classifications field.

Step 15 If you want to set a default classification for all packets on a VLAN, use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to all packets on a VLAN. The access point matches all packets with your class of service selection.

Step 16 Click the **Add** button beside the Class of Service menu for *Default classification for packets on the VLAN*. The classification appears in the Classifications field.

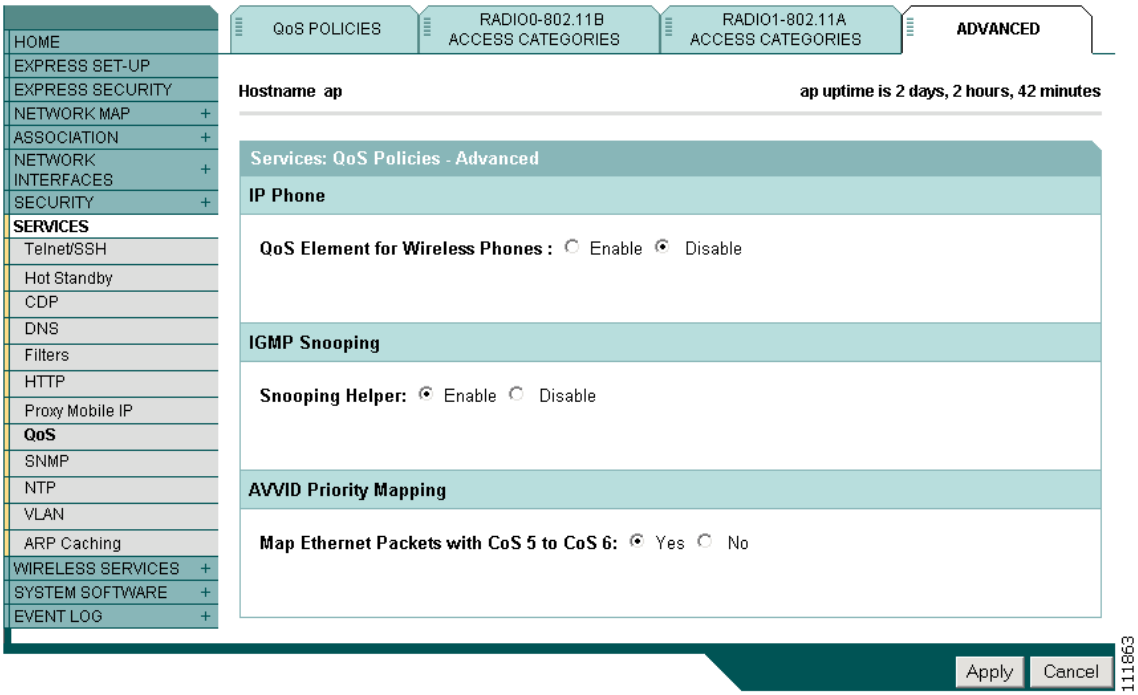
Step 17 When you finish adding classifications to the policy, click the **Apply** button under the Apply Class of Service drop-down menus. To cancel the policy and reset all fields to defaults, click the **Cancel** button under the Apply Class of Service drop-down menus. To delete the entire policy, click the **Delete** button under the Apply Class of Service drop-down menus.

Step 18 Use the Apply Policies to Interface/VLANs drop-down menus to apply policies to the access point Ethernet and radio ports. If VLANs are configured on the access point, drop-down menus for each VLAN's virtual ports appear in this section. If VLANs are not configured on the access point, drop-down menus for each interface appear.

Step 19 Click the **Apply** button at the bottom of the page to apply the policies to the access point ports.

Step 20 If you want the access point to give priority to all voice packets regardless of VLAN, click the **Advanced** tab. Figure 14-3 shows the QoS Policies - Advanced page.

Figure 14-3 QoS Policies - Advanced Page



Select **Enable** and click **Apply** to give top priority to all voice packets.

Note When you enable QoS Element for Wireless Phones, the access point gives top priority to voice packets even if you do not enable QoS. This setting operates independently from the QoS policies that you configure.

Adjusting Radio Access Categories

The access point uses the radio access categories to calculate backoff times for each packet. As a rule, high-priority packets have short backoff times.

The default values in the Min and Max Contention Window fields and in the Slot Time fields are based on settings recommended in IEEE Draft Standard 802.11e. For detailed information on these values, consult that standard.

We strongly recommend that you use the default settings on the Radio Access Categories page. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose. If you change these values and find that you need to reset them to defaults, use the default settings listed in Table 14-2.

The values listed in Table 14-2 are to the power of 2. The access point computes Contention Window values with this equation:

CW = 2 ** X minus 1

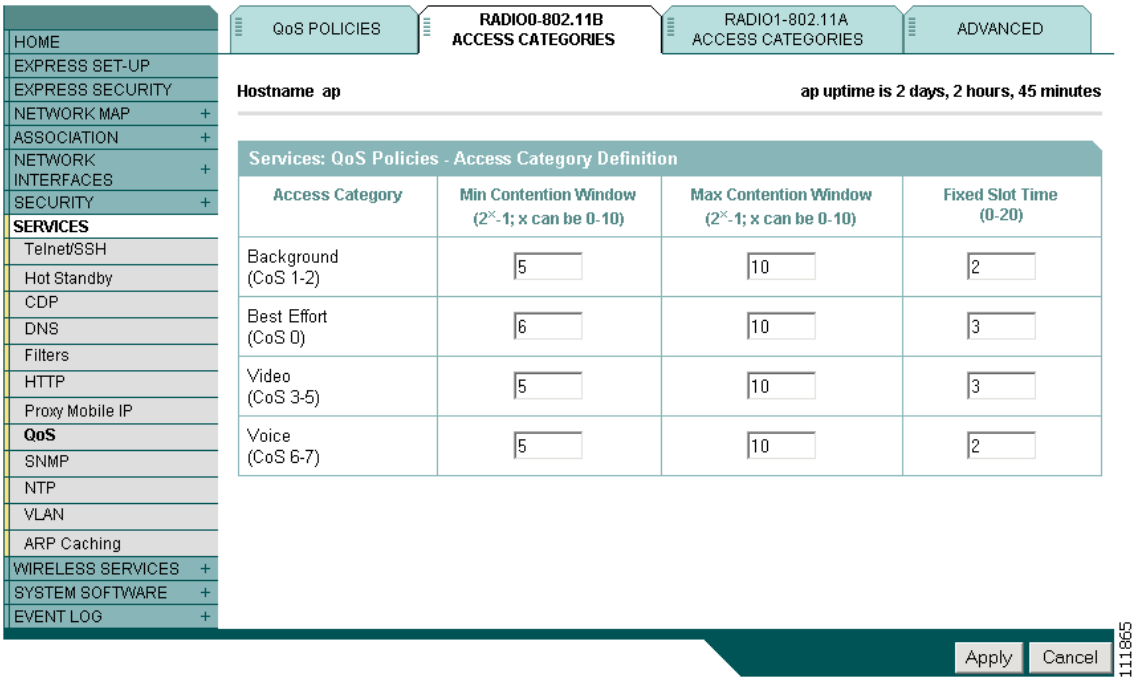
where X is the value from Table 14-2.

Table 14-2 Default QoS Radio Access Categories

Class of Service	Min Contention Window	Max Contention Window	Fixed Slot Time
Background	5	10	6
Best Effort	3	10	2
Video <100ms Latency	4	5	1
Voice <100ms Latency	3	4	1

Figure 14-4 shows the Radio Access Categories page. Dual-radio access points have a Radio Access Categories page for each radio.

Figure 14-4 Radio Access Categories Page



Disabling IGMP Snooping Helper

When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch and a client roams from one access point to another, the client's multicast session is dropped. When the access point's IGMP snooping helper is enabled, the access point sends a general IGMP query to the network infrastructure on behalf of the client every time the client associates or reassociates to the access point. By doing so, the multicast stream is maintained for the client as it roams.

The IGMP snooping helper is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select **Disable**, and click **Apply**. Figure 14-3 shows the QoS Policies - Advanced page.

Disabling AVVID Priority Mapping

AVVID priority mapping maps Ethernet packets tagged as class of service 5 to class of service 6. This feature enables the access point to apply the correct priority to voice packets for compatibility with Cisco AVVID networks.

AVVID priority mapping is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select **No** for Map Ethernet Packets with CoS 5 to CoS 6, and click **Apply**. Figure 14-3 shows the QoS Policies - Advanced page.

QoS Configuration Examples

These sections describe two common uses for QoS:

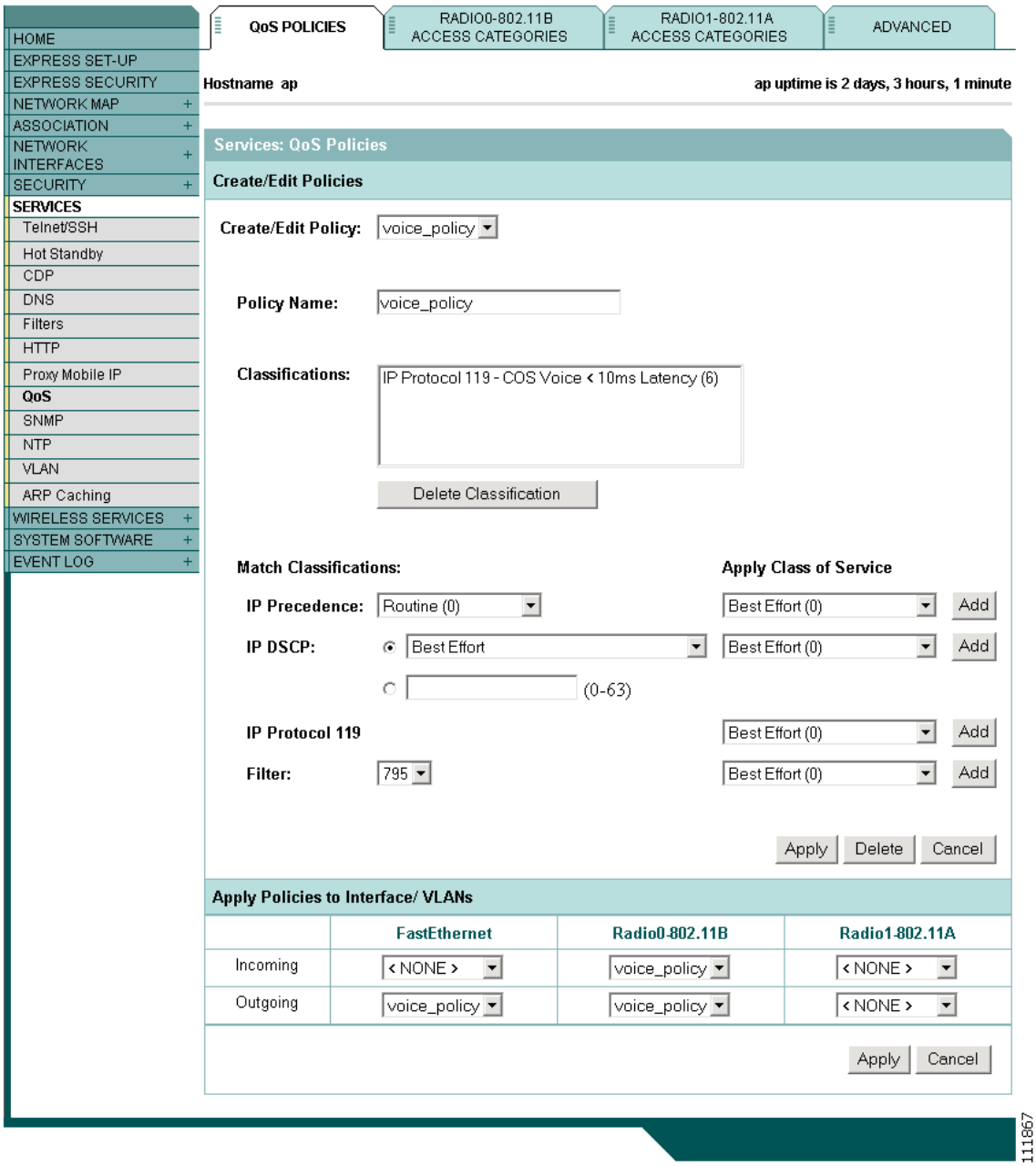
- Giving Priority to Voice Traffic, page 14-10
- Giving Priority to Video Traffic, page 14-12

Giving Priority to Voice Traffic

This section demonstrates how you can apply a QoS policy to your wireless network's voice VLAN to give priority to wireless phone traffic.

In this example, the network administrator creates a policy named *voice_policy* that applies voice class of service to traffic from Spectralink phones (protocol 119 packets). The user applies the voice_policy to the incoming and outgoing radio ports and to the outgoing Ethernet port. Figure 14-5 shows the administrator's QoS Policies page.

Figure 14-5 QoS Policies Page for Voice Example



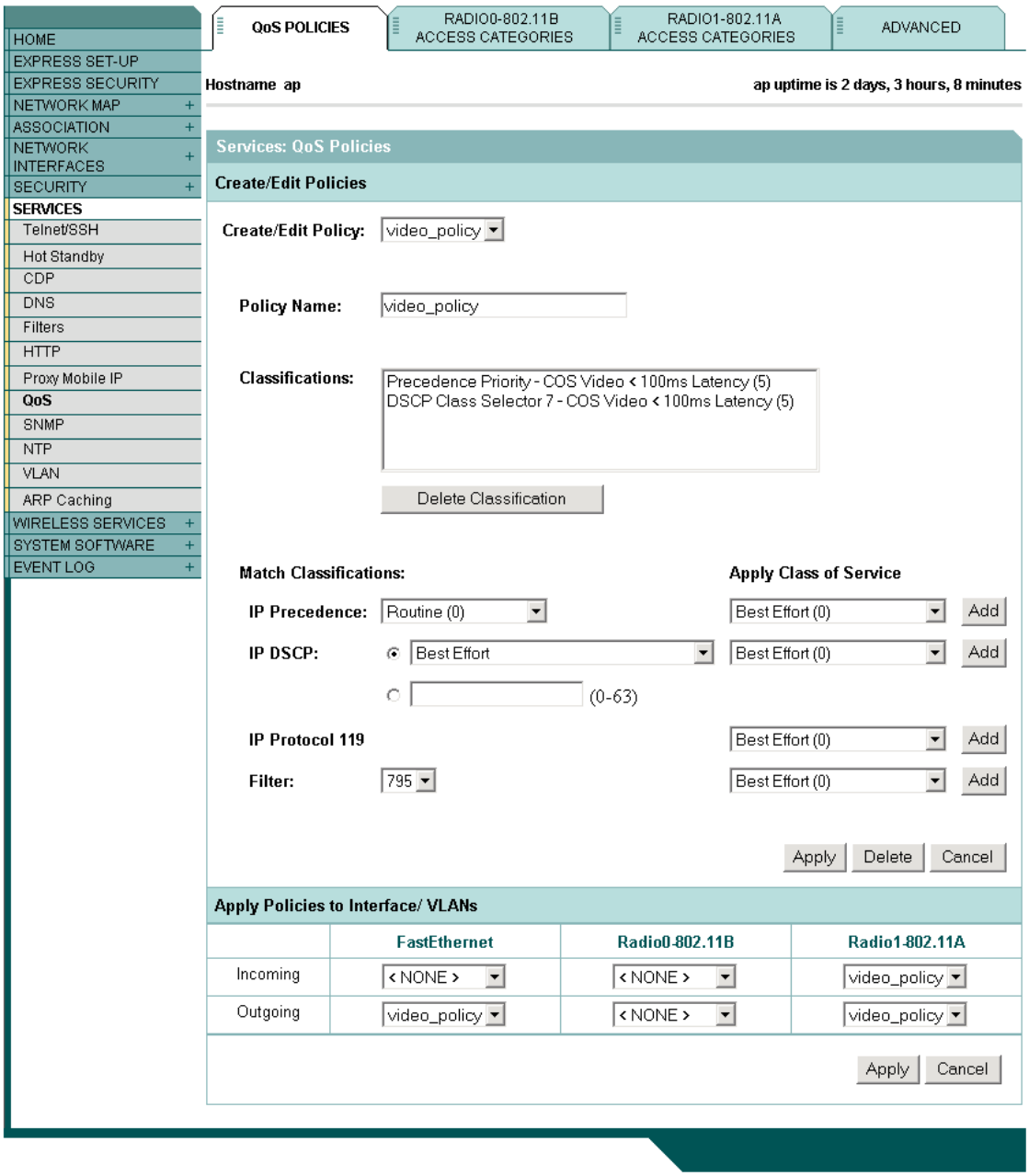
The network administrator also enables the *QoS element for wireless phones* setting on the QoS Policies - Advanced page. This setting gives priority to all voice traffic regardless of VLAN.

Giving Priority to Video Traffic

This section demonstrates how you could apply a QoS policy to a VLAN on your network dedicated to video traffic.

In this example, the network administrator creates a policy named *video_policy* that applies video class of service to video traffic. The user applies the video_policy to the incoming and outgoing radio ports and to the outgoing Ethernet port. Figure 14-6 shows the administrator's QoS Policies page.

Figure 14-6 QoS Policies Page for Video Example



Configuring Proxy Mobile IP

This chapter describes how to configure your access point's proxy Mobile IP feature. This chapter contains these sections:

- Understanding Proxy Mobile IP, page 15-2
- Configuring Proxy Mobile IP, page 15-6

Understanding Proxy Mobile IP

These sections explain how access points conduct proxy Mobile IP:

- Overview, page 15-2
- Components of a Proxy Mobile IP Network, page 15-2
- How Proxy Mobile IP Works, page 15-3
- Proxy Mobile IP Security, page 15-6

Overview

The access point's proxy Mobile IP feature works in conjunction with the Mobile IP feature in Cisco IOS software. When you enable proxy Mobile IP on your access point and on your wired network, the access point helps client devices from other networks remain connected to their home networks. The visiting client devices do not need special software; the access point provides proxy Mobile IP services on their behalf. Any wireless client can participate.

Mobile IP provides users the freedom to roam beyond their home subnets while maintaining their home IP addresses. This enables transparent routing of IP datagrams to mobile users during their movement, so that data sessions can be initiated to them while they roam. For example, a client device with an IP address of 192.95.5.2 could associate to an access point on a network whose IP addresses are in the 209.165.200.x range. The guest client device keeps its 192.95.5.2 IP address, and the access point forwards its packets through a Mobile IP enabled router across the Internet to a router on the client's home network.

Access points with proxy Mobile IP enabled attempt to provide proxy service for any client device that associates and does not perform the following:

- Does not issue a DHCP request to get a new IP address.
- Does not support a Mobile IP stack. If a device supports a Mobile IP stack, the access point assumes that the device will perform its own Mobile IP functions.

You enable proxy Mobile IP for specific SSIDs on the access point, providing support only for clients that use those SSIDs. Proxy Mobile IP does not support VLANs. You can pause proxy Mobile IP support without losing your proxy Mobile IP configuration.

Proxy Mobile IP is disabled by default.

Note Guest client devices do not receive broadcast and multicast packets.

Components of a Proxy Mobile IP Network

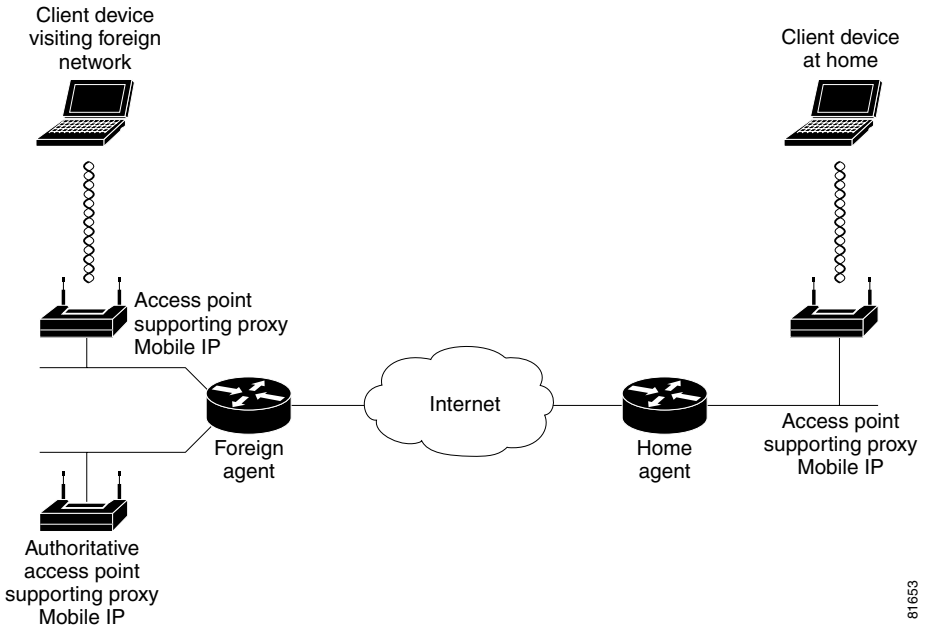
Five devices participate in proxy Mobile IP:

- A visiting client device. The visiting client device is any device such as a personal digital assistant or a laptop that can associate to a wireless access point. It does not need any special proxy Mobile IP software.
- An access point with proxy Mobile IP enabled. The access point proxies on behalf of the visiting client device, performing all Mobile IP services for the device.

- An authoritative access point on your network supporting proxy Mobile IP. The authoritative access point uses a subnet map to keep track of the home agent information for all visiting client devices.
- A home agent. The home agent is a router on the visiting client's home network that serves as the anchor point for communication with the access point and the visiting client. The home agent tunnels packets from a correspondent node on the Internet to the visiting client device.
- A foreign agent. The foreign agent is a router on your network that serves as the point of attachment for the visiting client device when it is on your network, delivering packets from the home agent to the visiting client.

Figure 15-1 shows the five participating devices.

Figure 15-1 Participating Devices in Proxy Mobile IP



How Proxy Mobile IP Works

The proxy Mobile IP process has four main phases. These sections describe each phase:

- Agent Discovery, page 15-3
- Subnet Map Exchange, page 15-4
- Registration, page 15-5
- Tunneling, page 15-5

Agent Discovery

During the agent discovery phase, the home agent and the foreign agent advertise their services on the network by using the ICMP Router Discovery Protocol (IRDP). The access point listens to these advertisements.

The IRDP advertisements carry Mobile IP extensions that specify whether an agent is a home agent, foreign agent, or both; its care-of address; the types of services it provides, such as reverse tunneling and generic routing encapsulation (GRE); and the allowed registration lifetime or roaming period for visiting client devices. Rather than waiting for agent advertisements, an access point can send out an agent solicitation. This solicitation forces any agents on the network to immediately send an agent advertisement.

When an access point determines that a client device is connected to a foreign network, it acquires a care-of address for the visiting client. The care-of address is an IP address of a foreign agent that has an interface on the network being visited by a client device. An access point can share this address among many visiting client devices.

When the visiting client associates to an access point, the access point compares the client's IP address with that of its own IP network information and detects that the client is a visitor from another network. The access point then begins the registration. However, before the access point can begin the registration process on behalf of the visiting client, it needs to know the home agent IP address of the visiting client. It gets the home agent's IP address by looking it up on a subnet map table.

Subnet Map Exchange

Each access point with proxy Mobile IP enabled maintains a subnet map table. The subnet map table consists of a list of home agent IP addresses and their subnet masks. Table 15-1 is an example of a subnet map table.

Table 15-1 Example of a Subnet Map Table

Home Agent	Subnet Mask
10.10.10.1	255.255.255.0
10.10.4.2	255.255.255.0
10.3.4.4	255.255.255.248
10.12.1.1	255.255.0.0

Access points use the subnet map table to determine the IP address of the visiting client's home agent. When an access point boots up or when proxy Mobile IP is first enabled on an access point, it obtains its own home agent information using the agent discovery mechanism. It sends this information to another access point called an authoritative access point (AAP). The AAP is an access point that is responsible for keeping the latest subnet map table.

When the AAP receives the new information, it replies to the access point with a copy of the latest subnet map table. The new access point now has the latest subnet map table locally and it is ready to perform proxy Mobile IP for visiting clients. Having the subnet map table locally helps the access point do a quick lookup for the home agent information. Meanwhile, the AAP adds the new access point to its list of access points and the home agent information to its subnet map table. The AAP then updates all the other access points with this additional piece of information.

You can designate up to three AAPs on your wireless LAN. If an access point fails to reach the first AAP, it tries the next configured AAP. The AAPs compare their subnet map tables periodically to make sure they have the same subnet map table. If the AAP detects that there are no more access points for a particular home agent, it sends a deregistration packet on behalf of the broadcast address of the home agent subnet to see if the home agent is still active. If the home agent responds, the AAP keeps the home agent entry in the subnet map table even though there are no access points in the home agent's subnet. This process supports client devices that have already roamed to foreign networks. If the home agent does not respond, the AAP deletes the home agent entry from the subnet map table.

When a client device associates to an access point and the access point determines that the client is visiting from another network, the access point performs a longest-match lookup on its subnet map table and obtains the home agent address for the visiting client. When the access point has the home agent address, it can proceed to the registration step.

Registration

The access point is configured with the mobility security association (which includes the shared key) of all potential visiting clients with their corresponding home agents. You can enter the mobility security association information locally on the access point or on a RADIUS server on your network, and access points with proxy Mobile IP enabled can access it there.

The access point uses the security association information, the visiting client's IP address, and the information that it learns from the foreign agent advertisements to form a Mobile IP registration request on behalf of the visiting client. It sends the registration request to the visiting client's home agent through the foreign agent. The foreign agent checks the validity of the registration request, which includes checking that the requested lifetime does not exceed its limitations and that the requested tunnel encapsulation is available. If the registration request is valid, the foreign agent relays the request to the home agent.

The home agent checks the validity of the registration request, which includes authentication of the visiting client. If the registration request is valid, the home agent creates a mobility binding (an association of the visiting client with its care-of address), a tunnel to the care-of address, and a routing entry for forwarding packets to the home address through the tunnel.

The home agent then sends a registration reply to the visiting client through the foreign agent (because the registration request was received through the foreign agent). The foreign agent checks the validity of the registration reply, including ensuring that an associated registration request exists in its pending list. If the registration reply is valid, the foreign agent adds the visiting client to its visitor list, establishes a tunnel to the home agent, and creates a routing entry for forwarding packets to the home address. It then relays the registration reply to the visiting client.

Finally, the access point checks the validity of the registration reply. If the registration reply specifies that the registration is accepted, the access point is able to confirm that the mobility agents are aware of the visiting client's roaming. Subsequently, the access point intercepts all packets from the visiting client and sends them to the foreign agent.

The access point re-registers on behalf of the visiting client before its registration lifetime expires. The home agent and foreign agent update their mobility binding and visitor entry, respectively, during re-registration.

A successful Mobile IP registration by the access point on behalf of the visiting client sets up the routing mechanism for transporting packets to and from the visiting client as it roams.

Tunneling

The visiting client sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the visiting client is roaming on foreign networks, its movements are transparent to correspondent nodes (other devices with which the visiting client communicates).

Data packets addressed to the visiting client are routed to its home network, where the home agent intercepts and tunnels them to the care-of address toward the visiting client. Tunneling has two primary functions: encapsulation of the data packet to reach the tunnel endpoint, and decapsulation when the packet is delivered at that endpoint. The tunnel mode that the access point supports is IPinIP Encapsulation.

Typically, the visiting client sends packets as it normally would. The access point intercepts these packets and sends them to the foreign agent, which routes them to their final destination, the correspondent node.

GRE Encapsulation

Instead of IPinIP Encapsulation, you can select GRE encapsulation. Use the **ip proxy-mobile tunnel gre** command to select GRE encapsulation.

Reverse Tunnels

Forward tunnels carry packets destined to the mobile node from the home network to the foreign network. You can also set up a reverse tunnel. A reverse tunnel carries packets between the home network and the foreign network, but it tunnels packets from the mobile node instead of packets to the mobile node. Therefore, instead of the foreign agent routing the packets from the mobile node normally, the foreign agent sends packets from the mobile node back to the home agent through the reverse tunnel. The home agent on the mobile node's home subnet routes the packets normally. Use the **ip proxy-mobile tunnel reverse** command to configure a reverse tunnel.

Proxy Mobile IP Security

Mobile IP uses a strong authentication scheme to protect communications to and from visiting clients. All registration messages between a visiting client and the home agent must contain the Mobile-Home Authentication Extension (MHAE). Proxy Mobile IP also implements this requirement in the registration messages sent by the access point on behalf of the visiting clients to the home agent.

The integrity of the registration messages is protected by a shared 128-bit key between the access point (on behalf of the visiting client) and the home agent. You can enter the shared key on the access point or on a RADIUS server.

The keyed message digest algorithm 5 (MD5) in prefix+suffix mode is used to compute the authenticator value in the appended MHAE. Mobile IP and proxy Mobile IP also support the hash-based message authentication code (HMAC-MD5). The receiver compares the authenticator value it computes over the message with the value in the extension to verify the authenticity.

Optionally, the Mobile-Foreign Authentication Extension and the Foreign-Home Authentication Extension are appended to protect message exchanges between a visiting client and foreign agent and between a foreign agent and home agent, respectively.

Replay protection uses the identification field in the registration messages as a timestamp and sequence number. The home agent returns its time stamp to synchronize the visiting client for registration. In proxy Mobile IP, the visiting clients are not synchronized to their home agents because the access point intercepts all home agent messages.

Configuring Proxy Mobile IP

These sections describe how to configure proxy Mobile IP:

- Configuration Guidelines, page 15-7
- Configuring Proxy Mobile IP on Your Wired LAN, page 15-7
- Configuring Proxy Mobile IP on Your Access Point, page 15-8

Configuration Guidelines

Before configuring proxy Mobile IP, you should consider these guidelines:

- You can enable proxy Mobile IP only on root access points (units connected to the wired LAN). You cannot enable proxy Mobile IP on repeater access points.
- Access points participating in proxy Mobile IP should be configured with gateway addresses. You can configure the gateways manually, or the access points can receive gateways through DHCP.
- The foreign and home agents must reside on the network gateways where you want to support proxy Mobile IP.
- If your authoritative access points receive their IP addresses through DHCP, use the access point host names to specify the AAPs in the proxy Mobile IP configuration.
- Proxy Mobile IP does not support broadcast and multicast traffic for visiting clients.
- To use proxy Mobile IP with DHCP-enabled client devices, you must disable Media Sense on the client devices. You can find instructions for disabling Media Sense in *Microsoft Knowledge Base Article Q239924*. Click this URL to browse to this article:

  http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q239924&
- Proxy Mobile IP does not support VLANs.
- If you disable proxy Mobile IP on your access point, the entire proxy Mobile IP configuration is cleared. To disable proxy Mobile IP without clearing the configuration, use the **ip proxy-mobile pause** command.

Configuring Proxy Mobile IP on Your Wired LAN

Proxy Mobile IP on access points works in conjunction with Mobile IP configured on your network routers. For instructions on configuring Mobile IP on a router on your network, refer to the Mobile IP chapter in *12.2 T New Features (Early Deployment Releases)*. Click this link to browse to the Mobile IP chapter:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm

Note To avoid problems with roaming client devices, you must configure two hidden global configuration mode commands on your Mobile IP router: **ip mobile bindupdate** and **ip mobile bindupdate ack**.

Configuring Proxy Mobile IP on Your Access Point

Beginning in privileged EXEC mode, follow these steps to configure proxy Mobile IP on your access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip proxy-mobile enable**	Enable proxy Mobile IP on the access point.
Step 3	**ip proxy-mobile aap** *ip-address* [*ip-address*] [*ip-address*]	Designate the access points that serve as the authoritative access points (the access points with which this access point compares its subnet table). **Note** You should specify at least two access points as AAPs in case one AAP fails. If you designate only one AAP and it goes offline, you lose all the information in the subnet map table.
Step 4	**ip proxy-mobile secure node** *address-start address-end* **spi** *spi* **key** { **hex** | **ascii** } *key*	Create security association settings for an IP address or for a range of IP addresses. • Enter an IP address, or the starting and ending addresses in an IP range. • Enter the security parameter index. • Enter a key for the security parameter. Specify whether the key contains hexadecimal or ASCII characters. If you choose hexadecimal, the key must contain 32 characters. If you choose ASCII, the key can contain up to 16 characters with no minimum length.
Step 5	**interface fastethernet 0**	Enter interface configuration mode for the Ethernet port.
Step 6	**ip proxy-mobile**	Enable proxy Mobile IP on the Ethernet port.
Step 7	**exit**	Return to global config mode.
Step 8	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio port. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 9	**ip proxy-mobile**	Enable proxy Mobile IP on the radio port.
Step 10	**ssid** *ssid*	Enter an SSID for which you want to enable proxy Mobile IP. **Note** Proxy Mobile IP functionality is not supported on SSIDs where VLAN is also enabled.
Step 11	**ip proxy-mobile**	Enable proxy Mobile IP for the SSID.
Step 12	**exit**	Return to global config mode.
Step 13	**interface bvi1**	Enter interface configuration mode for the bridge virtual interface (BVI).
Step 14	**ip proxy-mobile**	Enable proxy Mobile IP on the BVI.
Step 15	**end**	Return to privileged EXEC mode.
Step 16	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the ip proxy-mobile commands to disable proxy Mobile IP. Use the **ip proxy-mobile pause** command to disable proxy Mobile IP without losing your proxy Mobile IP configuration.

This example shows how to enable proxy Mobile IP on an access point for the SSID *tsunami* for IP addresses from 10.91.7.151 to 10.91.7.176:

```
ap1200# configure terminal
ap1200(config)# ip proxy-mobile enable
ap1200(config)# ip proxy-mobile aap 192.168.15.22 192.168.15.24 192.168.15.28
ap1200(config)# ip proxy-mobile secure node 10.91.7.151 10.91.7.176 spi 102 key ascii
0987654
ap1200(config)# interface fastethernet 0
ap1200(config-if)# ip proxy-mobile
ap1200(config-if)# interface dot11radio 0
ap1200(config-if)# ip proxy-mobile
ap1200(config-if)# ssid tsunami
ap1200(config-if-ssid)# ip proxy-mobile
ap1200(config-if-ssid)# exit
ap1200(config-if)# exit
ap1200(config)# interface bvi1
ap1200(config-if)# ip proxy-mobile
ap1200(config-if-ssid)# end
```

CHAPTER 16

Configuring Filters

This chapter describes how to configure and manage MAC address, IP, and Ethertype filters on the access point using the web-browser interface. This chapter contains these sections:

- Understanding Filters, page 16-2
- Configuring Filters Using the CLI, page 16-2
- Configuring Filters Using the Web-Browser Interface, page 16-2

Understanding Filters

Protocol filters (IP protocol, IP port, and Ethertype) prevent or allow the use of specific protocols through the access point's Ethernet and radio ports. You can set up individual protocol filters or sets of filters. You can filter protocols for wireless client devices, users on the wired LAN, or both. For example, an SNMP filter on the access point's radio port prevents wireless client devices from using SNMP with the access point but does not block SNMP access from the wired LAN.

IP address and MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific IP or MAC addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify.

You can configure filters using the web-browser interface or by entering commands in the CLI.

Note Using the CLI, you can configure up to 2,048 MAC addresses for filtering. Using the web-browser interface, however, you can configure only up to 43 MAC addresses for filtering.

Tip You can include filters in the access point's QoS policies. Refer to Chapter 14, "Configuring QoS," for detailed instructions on setting up QoS policies.

Configuring Filters Using the CLI

To configure filters using CLI commands, you use access control lists (ACLs) and bridge groups. You can find explanations of these concepts and instructions for implementing them in these documents:

- *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*. Click this link to browse to the "Configuring Transparent Bridging" chapter: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart1/bcftb.htm
- *Catalyst 4908G-L3 Cisco IOS Release 12.0(10)W5(18e) Software Feature and Configuration Guide*. Click this link to browse to the "Command Reference" chapter: http://www.cisco.com/univercd/cc/td/doc/product/l3sw/4908g_l3/ios_12/10w518e/config/cmd_ref.htm

Configuring Filters Using the Web-Browser Interface

This section describes how to configure and enable filters using the web-browser interface. You complete two steps to configure and enable a filter:

1. Name and configure the filter using the filter setup pages.
2. Enable the filter using the Apply Filters page.

These sections describe setting up and enabling three filter types:

- Configuring and Enabling MAC Address Filters, page 16-3
- Configuring and Enabling IP Filters, page 16-8
- Configuring and Enabling Ethertype Filters, page 16-11

Configuring and Enabling MAC Address Filters

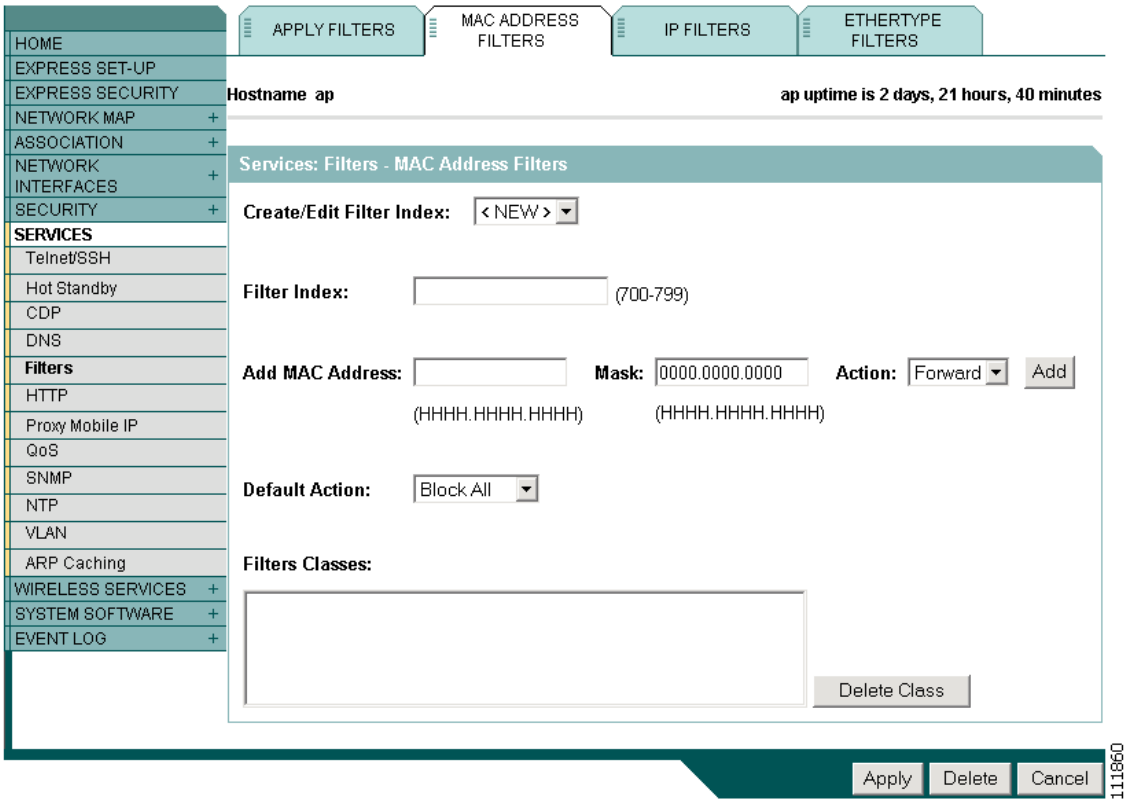
MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Note Using the CLI, you can configure up to 2,048 MAC addresses for filtering. Using the web-browser interface, however, you can configure only up to 43 MAC addresses for filtering.

Note MAC address filters are powerful, and you can lock yourself out of the access point if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point, use the CLI to disable the filters.

Use the MAC Address Filters page to create MAC address filters for the access point. Figure 16-1 shows the MAC Address Filters page.

Figure 16-1 MAC Address Filters Page



Follow this link path to reach the Address Filters page:

1. Click **Services** in the page navigation bar.

2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **MAC Address Filters** tab at the top of the page.

Creating a MAC Address Filter

Follow these steps to create a MAC address filter:

Step 1 Follow the link path to the MAC Address Filters page.

Step 2 If you are creating a new MAC address filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit a filter, select the filter number from the Create/Edit Filter Index menu.

Step 3 In the Filter Index field, name the filter with a number from 700 to 799. The number you assign creates an access control list (ACL) for the filter.

Step 4 Enter a MAC address in the Add MAC Address field. Enter the address with periods separating the three groups of four characters (0005.9a39.2110, for example).

Note To make sure the filter operates properly, use lower case for all the letters in the MAC addresses that you enter.

Step 5 Use the Mask entry field to indicate how many bits, from left to right, the filter checks against the MAC address. For example, to require an exact match with the MAC address (to check all bits) enter **0000.0000.0000**. To check only the first 4 bytes, enter **0.0.FFFF**.

Step 6 Select **Forward** or **Block** from the Action menu.

Step 7 Click **Add**. The MAC address appears in the Filters Classes field. To remove the MAC address from the Filters Classes list, select it and click **Delete Class**.

Step 8 Repeat Step 4 through Step 7 to add addresses to the filter.

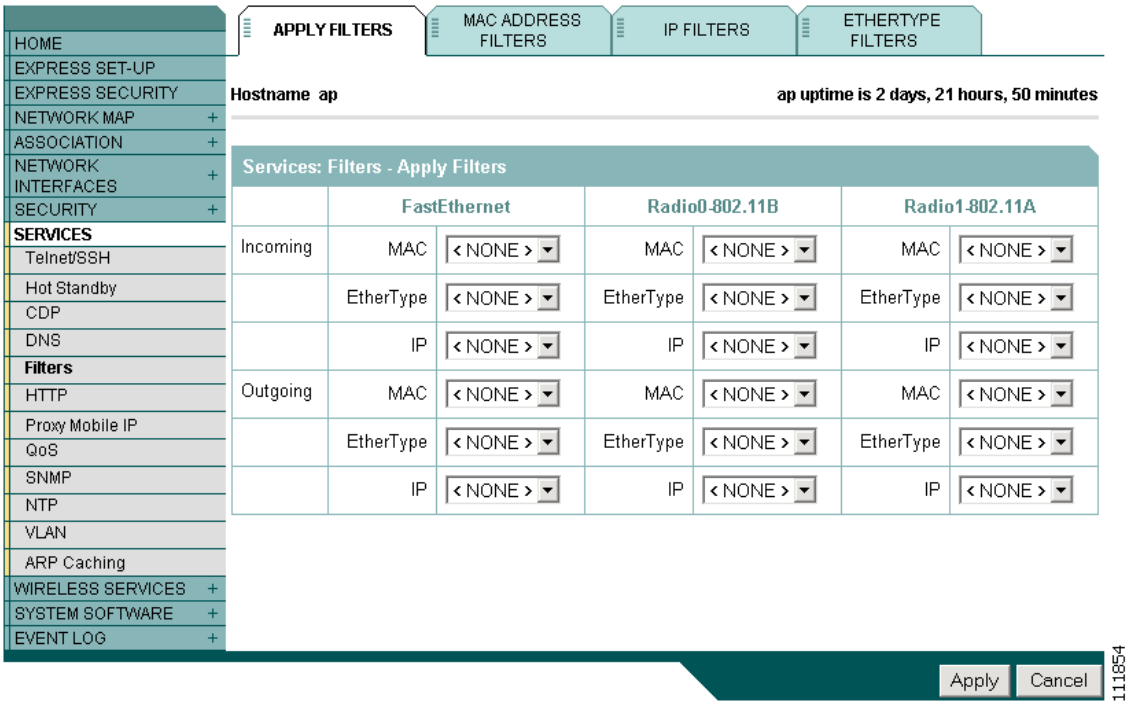
Step 9 Select **Forward All** or **Block All** from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you enter several addresses and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.

Tip You can create a list of allowed MAC addresses on an authentication server on your network. Consult the "Configuring Authentication Types" section on page 10-10 for instructions on using MAC-based authentication.

Step 10 Click **Apply**. The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.

Step 11 Click the **Apply Filters** tab to return to the Apply Filters page. Figure 16-2 shows the Apply Filters page.

Figure 16-2 Apply Filters Page



Step 12 Select the filter number from one of the MAC drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

Step 13 Click **Apply**. The filter is enabled on the selected ports.

If clients are not filtered immediately, click **Reload** on the System Configuration page to restart the access point. To reach the System Configuration page, click **System Software** on the task menu and then click **System Configuration**.

Note Client devices with blocked MAC addresses cannot send or receive data through the access point, but they might remain in the Association Table as unauthenticated client devices. Client devices with blocked MAC addresses disappear from the Association Table when the access point stops monitoring them, when the access point reboots, or when the clients associate to another access point.

Using MAC Address ACLs to Block or Allow Client Association to the Access Point

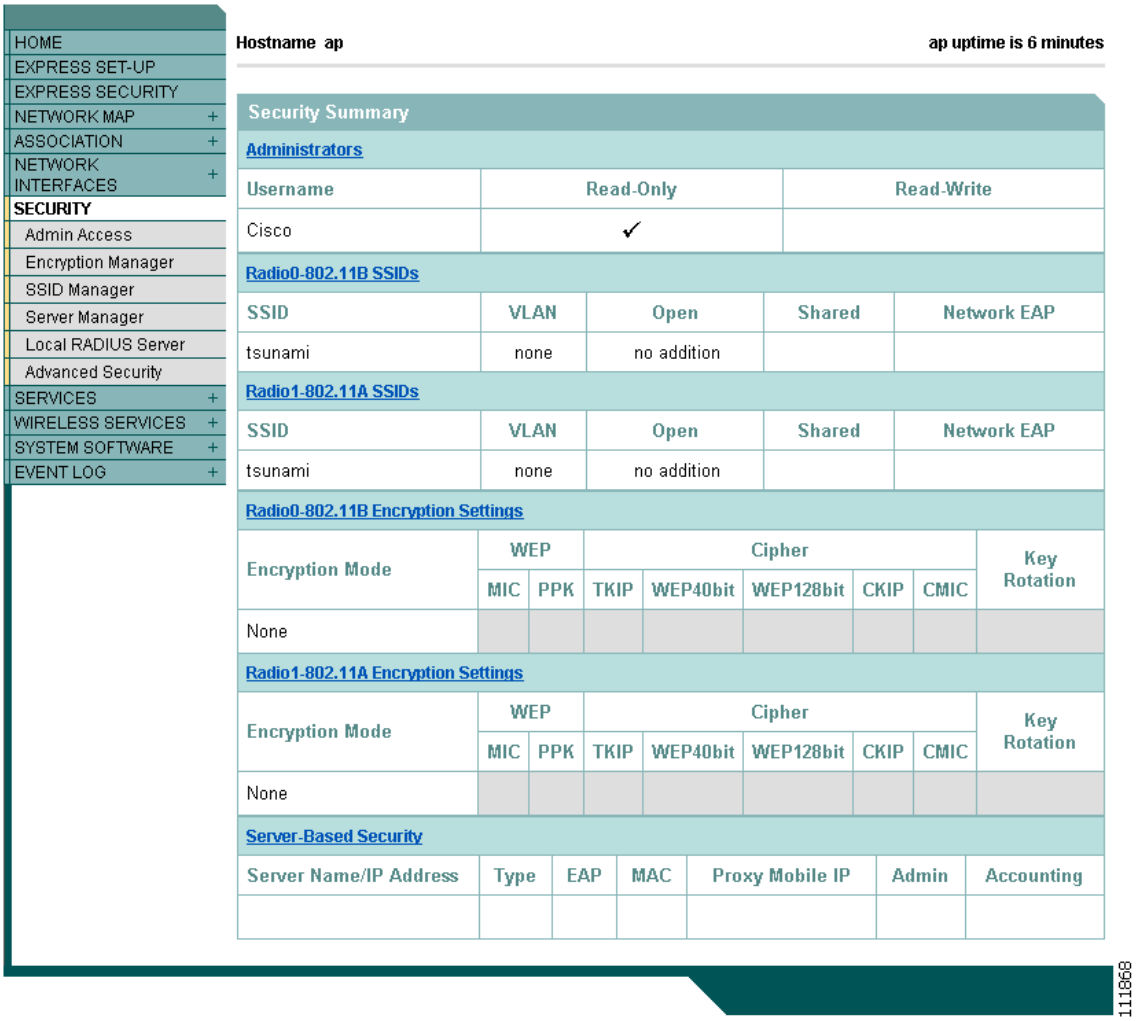
You can use MAC address ACLs to block or allow association to the access point. Instead of filtering traffic across an interface, you use the ACL to filter associations to the access point radio.

Follow these steps to use an ACL to filter associations to the access point radio:

Step 1 Follow Steps 1 through 10 in the "Creating a MAC Address Filter" section on page 16-4 to create an ACL. For MAC addresses that you want to allow to associate, select **Forward** from the Action menu. Select **Block** for addresses that you want to prevent from associating. Select **Block All** from the Default Action menu.

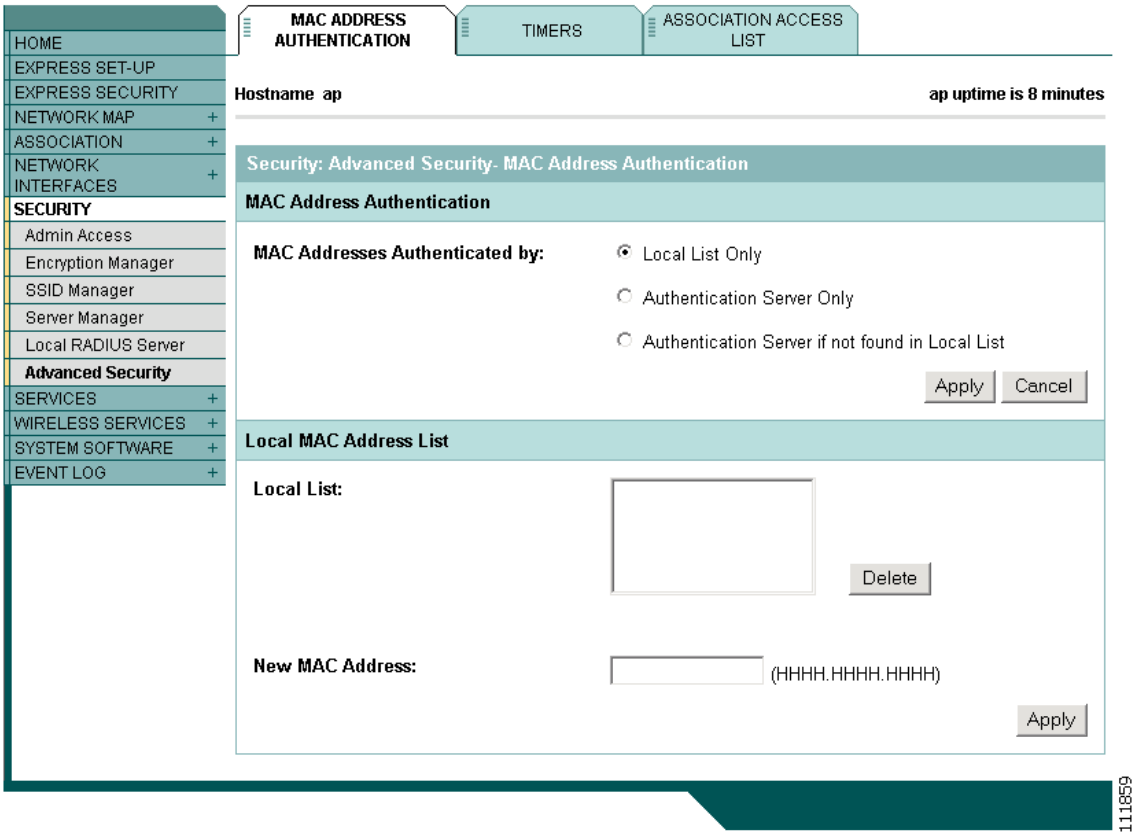
Step 2 Click **Security** to browse to the Security Summary page. Figure 16-3 shows the Security Summary page.

Figure 16-3 Security Summary Page



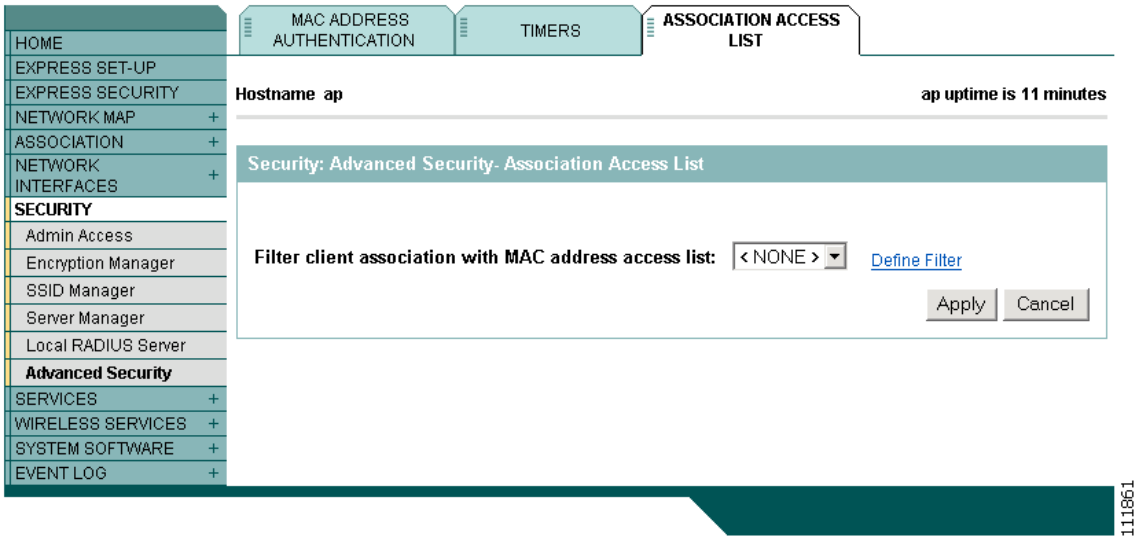
Step 3 Click **Advanced Security** to browse to the Advanced Security: MAC Address Authentication page. Figure 16-4 shows the MAC Address Authentication page.

Figure 16-4 Advanced Security: MAC Address Authentication Page



Step 4 Click the **Association Access List** tab to browse to the Association Access List page. Figure 16-5 shows the Association Access List page.

Figure 16-5 Association Access List Page



Step 5 Select your MAC address ACL from the drop-down menu.

Step 6 Click **Apply**.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Using MAC Address ACLs to Block or Allow Client Association to the Access Point" section on page 16-5:

```
AP# configure terminal
AP(config)# dot11 association access-list 777
AP(config)# end
```

In this example, only client devices with MAC addresses listed in access list 777 are allowed to associate to the access point. The access point blocks associations from all other MAC addresses.

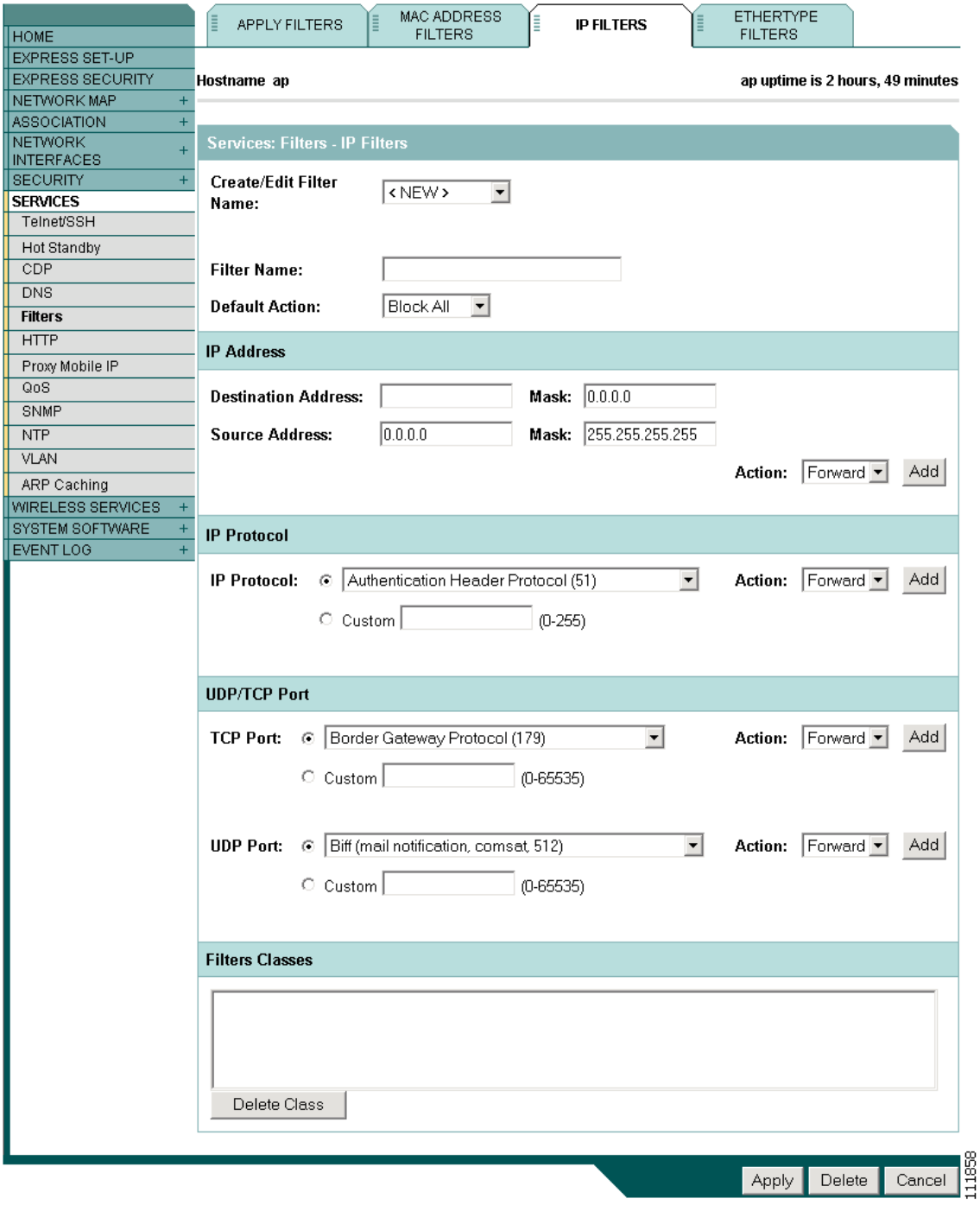
For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring and Enabling IP Filters

IP filters (IP address, IP protocol, and IP port) prevent or allow the use of specific protocols through the access point's Ethernet and radio ports, and IP address filters allow or prevent the forwarding of unicast and multicast packets either sent from or addressed to specific IP addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify. You can create filters that contain elements of one, two, or all three IP filtering methods. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the IP Filters page to create IP filters for the access point. Figure 16-6 shows the IP Filters page.

Figure 16-6 IP Filters Page



Follow this link path to reach the IP Filters page:

1. Click **Services** in the page navigation bar.

2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **IP Filters** tab at the top of the page.

Creating an IP Filter

Follow these steps to create an IP filter:

Step 1 Follow the link path to the IP Filters page.

Step 2 If you are creating a new filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit an existing filter, select the filter name from the Create/Edit Filter Index menu.

Step 3 Enter a descriptive name for the new filter in the Filter Name field.

Step 4 Select **Forward all** or **Block all** as the filter's default action from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you create a filter containing an IP address, an IP protocol, and an IP port and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.

Step 5 To filter an IP address, enter an address in the IP Address field.

Note If you plan to block traffic to all IP addresses except those you specify as allowed, put the address of your own PC in the list of allowed addresses to avoid losing connectivity to the access point.

Step 6 Type the mask for the IP address in the Mask field. Enter the mask with periods separating the groups of characters (112.334.556.778, for example). If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field. The mask you enter in this field behaves the same way that a mask behaves when you enter it in the CLI.

Step 7 Select **Forward** or **Block** from the Action menu.

Step 8 Click **Add**. The address appears in the Filters Classes field. To remove the address from the Filters Classes list, select it and click **Delete Class**. Repeat Step 5 through Step 8 to add addresses to the filter.

If you do not need to add IP protocol or IP port elements to the filter, skip to Step 15 to save the filter on the access point.

Step 9 To filter an IP protocol, select one of the commmon protocols from the IP Protocol drop-down menu, or select the **Custom** radio button and enter the number of an existing ACL in the Custom field. Enter an ACL number from 0 to 255. See Appendix B, "Protocol Filters," for a list of IP protocols and their numeric designators.

Step 10 Select **Forward** or **Block** from the Action menu.

Step 11 Click **Add**. The protocol appears in the Filters Classes field. To remove the protocol from the Filters Classes list, select it and click **Delete Class**. Repeat Step 9 to Step 11 to add protocols to the filter.

If you do not need to add IP port elements to the filter, skip to Step 15 to save the filter on the access point.

Step 12 To filter a TCP or UDP port protocol, select one of the commmon port protocols from the TCP Port or UDP Port drop-down menus, or select the **Custom** radio button and enter the number of an existing protocol in one of the Custom fields. Enter a protocol number from 0 to 65535. See Appendix B, "Protocol Filters," for a list of IP port protocols and their numeric designators.

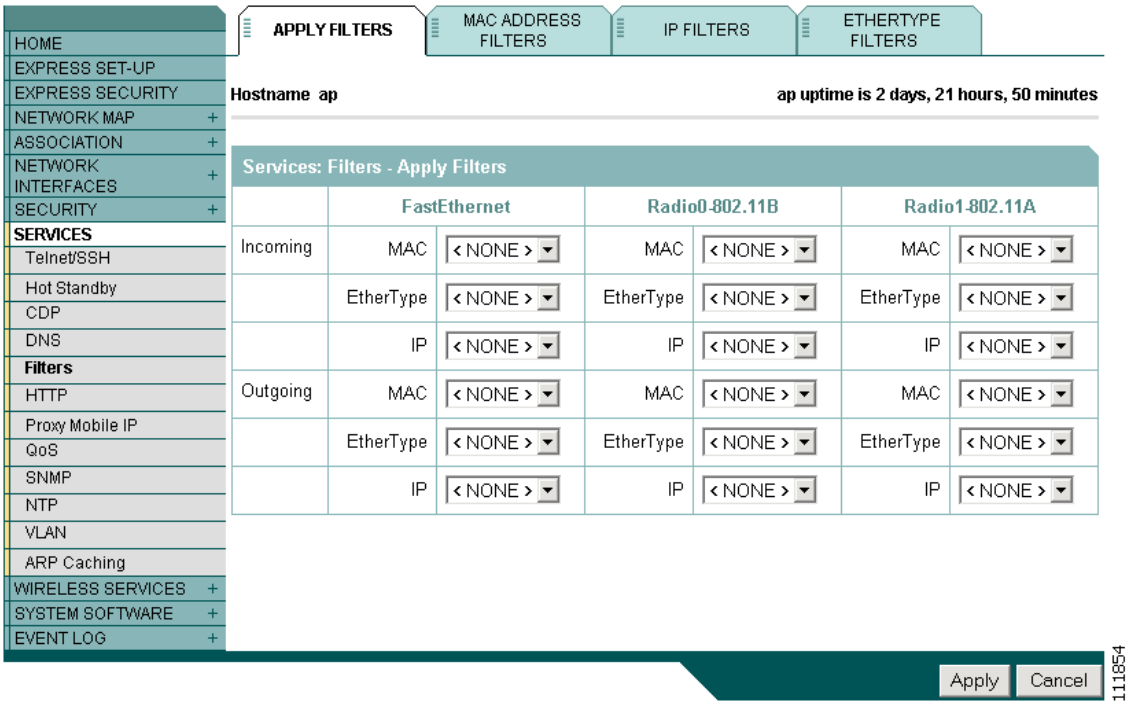
Step 13 Select **Forward** or **Block** from the Action menu.

Step 14 Click **Add**. The protocol appears in the Filters Classes field. To remove the protocol from the Filters Classes list, select it and click **Delete Class**. Repeat Step 12 to Step 14 to add protocols to the filter.

Step 15 When the filter is complete, click **Apply**. The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.

Step 16 Click the **Apply Filters** tab to return to the Apply Filters page. Figure 16-7 shows the Apply Filters page.

Figure 16-7 Apply Filters Page



Step 17 Select the filter name from one of the IP drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

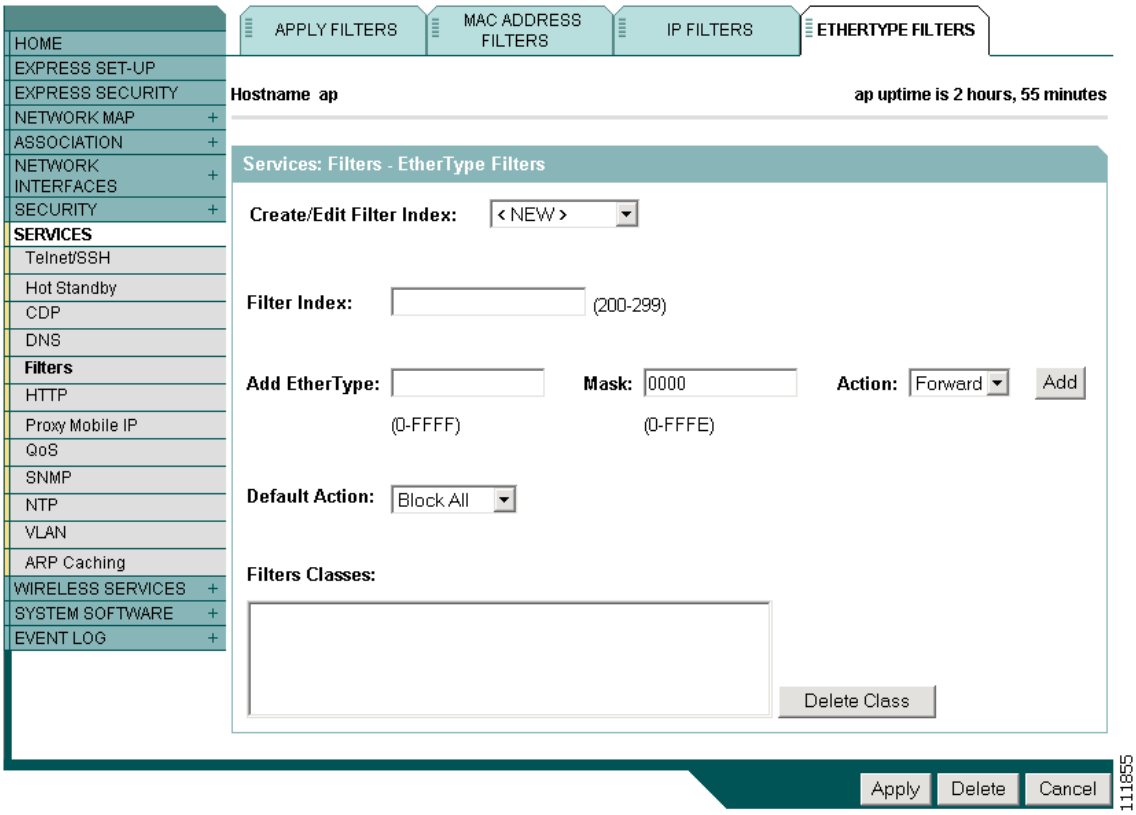
Step 18 Click **Apply**. The filter is enabled on the selected ports.

Configuring and Enabling Ethertype Filters

Ethertype filters prevent or allow the use of specific protocols through the access point's Ethernet and radio ports. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the Ethertype Filters page to create Ethertype filters for the access point. Figure 16-8 shows the Ethertype Filters page.

Figure 16-8 Ethertype Filters Page



Follow this link path to reach the Ethertype Filters page:

1. Click **Services** in the page navigation bar.
2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **Ethertype Filters** tab at the top of the page.

Creating an Ethertype Filter

Follow these steps to create an Ethertype filter:

Step 1 Follow the link path to the Ethertype Filters page.

Step 2 If you are creating a new filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit an existing filter, select the filter number from the Create/Edit Filter Index menu.

Step 3 In the Filter Index field, name the filter with a number from 200 to 299. The number you assign creates an access control list (ACL) for the filter.

Step 4 Enter an Ethertype number in the Add Ethertype field. See Appendix B, "Protocol Filters," for a list of protocols and their numeric designators.

Step 5 Enter the mask for the Ethertype in the Mask field. If you enter **0**, the mask requires an exact match of the Ethertype.

Step 6 Select **Forward** or **Block** from the Action menu.

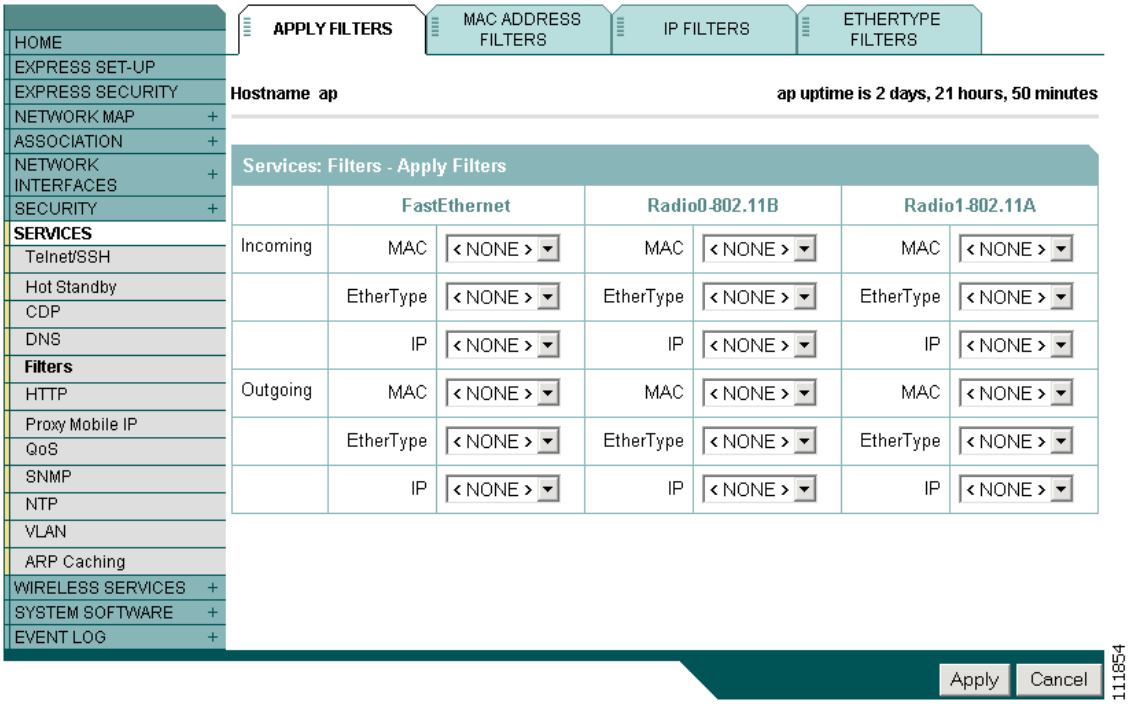
Step 7 Click **Add**. The Ethertype appears in the Filters Classes field. To remove the Ethertype from the Filters Classes list, select it and click **Delete Class**. Repeat Step 4 through Step 7 to add Ethertypes to the filter.

Step 8 Select **Forward All** or **Block All** from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the Ethertypes in the filter. For example, if you enter several Ethertypes and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.

Step 9 Click **Apply**. The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.

Step 10 Click the **Apply Filters** tab to return to the Apply Filters page. Figure 16-9 shows the Apply Filters page.

Figure 16-9 Apply Filters Page



Step 11 Select the filter number from one of the Ethertype drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

Step 12 Click **Apply**. The filter is enabled on the selected ports.

CHAPTER 17

Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on your access point.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco Aironet 1200 Series Access Point Command Reference* for this release and the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This chapter contains these sections:

- Understanding CDP, page 17-2
- Configuring CDP, page 17-2
- Monitoring and Maintaining CDP, page 17-4

Understanding CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices. Information in CDP packets is used in network management software such as CiscoWorks2000.

CDP is enabled on the access point's Ethernet port by default. However, CDP is enabled on the access point's radio port only when the radio is associated to another wireless infrastructure device, such as an access point or a bridge.

Note For best performance on your wireless LAN, disable CDP on all radio interfaces and on sub-interfaces if VLANs are enabled on the access point.

Configuring CDP

This section contains CDP configuration information and procedures:

- Default CDP Configuration, page 17-2
- Configuring the CDP Characteristics, page 17-2
- Disabling and Enabling CDP, page 17-3
- Disabling and Enabling CDP on an Interface, page 17-4

Default CDP Configuration

Table 17-1 lists the default CDP settings.

Table 17-1 Default CDP Configuration

Feature	Default Setting
CDP global state	Enabled
CDP interface state	Enabled
CDP holdtime (packet holdtime in seconds)	180
CDP timer (packets sent every x seconds)	60

Configuring the CDP Characteristics

You can configure the CDP holdtime (the number of seconds before the access point discards CDP packets) and the CDP timer (the number of seconds between each CDP packets the access point sends).

Beginning in Priveleged Exec mode, follow these steps to configure the CDP holdtime and CDP timer.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cdp holdtime** *seconds*	(Optional) Specify the amount of time a receiving device should hold the information sent by your device before discarding it. The range is from 10 to 255 seconds; the default is 180 seconds.
Step 3	**cdp timer** *seconds*	(Optional) Set the transmission frequency of CDP updates in seconds. The range is from 5 to 254; the default is 60 seconds.
Step 4	**end**	Return to Privileged Exec mode.

Use the **no** form of the CDP commands to return to the default settings.

This example shows how to configure and verify CDP characteristics:

```
AP# configure terminal
AP(config)# cdp holdtime 120
AP(config)# cdp timer 50
AP(config)# end

AP# show cdp

Global CDP information:
        Sending a holdtime value of 120 seconds
        Sending CDP packets every 50 seconds
```

For additional CDP **show** commands, see the "Monitoring and Maintaining CDP" section on page 17-4.

Disabling and Enabling CDP

CDP is enabled by default. Beginning in Priveleged Exec mode, follow these steps to disable the CDP device discovery capability.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no cdp run**	Disable CDP.
Step 3	**end**	Return to Privileged Exec mode.

Beginning in privileged EXEC mode, follow these steps to enable CDP:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cdp run**	Enable CDP after disabling it.
Step 3	**end**	Return to privileged EXEC mode.

This example shows how to enable CDP.

```
AP# configure terminal
AP(config)# cdp run
AP(config)# end
```

Disabling and Enabling CDP on an Interface

CDP is enabled by default on all supported interfaces to send and receive CDP information.

Beginning in privileged EXEC mode, follow these steps to disable CDP on an interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the interface on which you are disabling CDP.
Step 3	**no cdp enable**	Disable CDP on an interface.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Beginning in privileged EXEC mode, follow these steps to enable CDP on an interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the interface on which you are enabling CDP.
Step 3	**cdp enable**	Enable CDP on an interface after disabling it.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to enable CDP on an interface.

```
AP# configure terminal
AP(config)# interface x
AP(config-if)# cdp enable
AP(config-if)# end
```

Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, perform one or more of these tasks, beginning in privileged EXEC mode.

Command	Description
clear cdp counters	Reset the traffic counters to zero.
clear cdp table	Delete the CDP table of information about neighbors.

Command	Description
show cdp	Display global information, such as frequency of transmissions and the holdtime for packets being sent.
show cdp entry *entry-name* [**protocol** | **version**]	Display information about a specific neighbor. You can enter an asterisk (*) to display all CDP neighbors, or you can enter the name of the neighbor about which you want information. You can also limit the display to information about the protocols enabled on the specified neighbor or information about the version of software running on the device.
show cdp interface [*type number*]	Display information about interfaces where CDP is enabled. You can limit the display to the type of interface or the number of the interface about which you want information (for example, entering **gigabitethernet 0/1** displays information only about Gigabit Ethernet port 1).
show cdp neighbors [*type number*] [**detail**]	Display information about neighbors, including device type, interface type and number, holdtime settings, capabilities, platform, and port ID. You can limit the display to neighbors on a specific type or number of interface or expand the display to provide more detailed information.
show cdp traffic	Display CDP counters, including the number of packets sent and received and checksum errors.

Below are six examples of output from the CDP **show** privileged EXEC commands:

```
AP# show cdp

Global CDP information:
        Sending CDP packets every 50 seconds
        Sending a holdtime value of 120 seconds

AP# show cdp entry *
-------------------------
Device ID: AP
Entry address(es):
  IP address: 10.1.1.66
Platform: cisco WS-C3550-12T,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/2,  Port ID (outgoing port): GigabitEthernet0/2
Holdtime : 129 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Experimental Version 12.1(20010612:021
316) [jang-flamingo 120]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 06-Jul-01 18:18 by jang

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=0000000
0FFFFFFFF010221FF0000000000000000024B293A00FF0000
VTP Management Domain: ''
Duplex: full

-------------------------
Device ID: idf2-1-lab-13.cisco.com
Entry address(es):
  IP address: 10.1.1.10
Platform: cisco WS-C3524-XL,  Capabilities: Trans-Bridge Switch
```

```
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/10
Holdtime : 141 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.1)XP, MAINTENANCE IN
TERIM SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Fri 10-Dec-99 11:16 by cchang

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=25, value=0000000
0FFFFFFFF010101FF00000000000000000142EFA400FF
VTP Management Domain: ''

AP# show cdp entry * protocol
Protocol information for talSwitch14 :
  IP address: 172.20.135.194
Protocol information for tstswitch2 :
  IP address: 172.20.135.204
  IP address: 172.20.135.202
Protocol information for tstswitch2 :
  IP address: 172.20.135.204
  IP address: 172.20.135.202

AP# show cdp interface
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/2 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/3 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/4 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/5 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/6 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/7 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/8 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

AP# show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce       Holdtme      Capability     Platform       Port ID
```

```
Perdido2         Gig 0/6             125          R S I          WS-C3550-1Gig       0/6
Perdido2         Gig 0/5             125          R S I          WS-C3550-1Gig       0/5

AP# show cdp traffic
CDP counters :
        Total packets output: 50882, Input: 52510
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 50882, Input: 52510
```

CHAPTER 18

Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on your access point.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release and to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This chapter consists of these sections:

- Understanding SNMP, page 18-2
- Configuring SNMP, page 18-4
- Displaying SNMP Status, page 18-10

Understanding SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and management information base (MIB) reside on the access point. To configure SNMP on the access point, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

This section includes these concepts:

- SNMP Versions, page 18-2
- SNMP Manager Functions, page 18-3
- SNMP Agent Functions, page 18-3
- SNMP Community Strings, page 18-3
- Using SNMP to Access MIB Variables, page 18-4

SNMP Versions

This software release supports these SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a full Internet standard, defined in RFC 1157.
- SNMPv2C, which has these features:
  - SNMPv2—Version 2 of the Simple Network Management Protocol, a draft Internet standard, defined in RFCs 1902 through 1907.
  - SNMPv2C—The Community-based Administrative Framework for SNMPv2, an experimental Internet protocol defined in RFC 1901.

SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the Community-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; therefore, you can configure the software to support communications with one management station using the SNMPv1 protocol and another using the SNMPv2 protocol.

SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in Table 18-1.

Table 18-1 SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table.[1]
get-bulk-request[2]	Retrieves large blocks of data that would otherwise require the transmission of many small blocks of data, such as multiple rows in a table.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

1. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
2. The **get-bulk** command works only with SNMPv2.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the access point, the community string definitions on the NMS must match at least one of the three community string definitions on the access point.

A community string can have one of these attributes:

- Read-only—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access

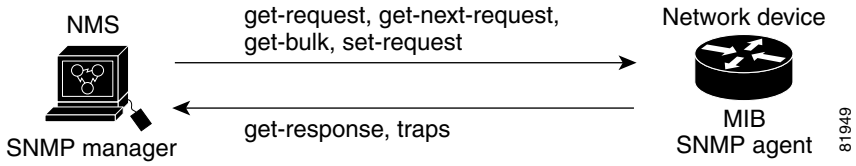
- Read-write—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

Using SNMP to Access MIB Variables

An example of an NMS is the CiscoWorks network management software. CiscoWorks 2000 software uses the access point MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in Figure 18-1, the SNMP agent gathers data from the MIB. The agent can send traps (notification of certain events) to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

Figure 18-1 SNMP Network



For information on supported MIBs and how to access them, see Appendix C, "Supported MIBs."

Configuring SNMP

This section describes how to configure SNMP on your access point. It contains this configuration information:

- Default SNMP Configuration, page 18-5
- Enabling the SNMP Agent, page 18-5
- Configuring Community Strings, page 18-5
- Configuring Trap Managers and Enabling Traps, page 18-7
- Setting the Agent Contact and Location Information, page 18-9
- Using the snmp-server view Command, page 18-9
- SNMP Examples, page 18-9

Default SNMP Configuration

Table 18-2 shows the default SNMP configuration.

Table 18-2 Default SNMP Configuration

Feature	Default Setting
SNMP agent	Disabled
SNMP community strings	No strings are configured by default. However, when you enable SNMP using the web-browser interface, the access point automatically creates the *public* community with read-only access to the IEEE802dot11 MIB.
SNMP trap receiver	None configured
SNMP traps	None enabled

Enabling the SNMP Agent

No specific CLI command exists to enable SNMP. The first **snmp-server** global configuration command that you enter enables SNMPv1 and SNMPv2.

You can also enable SNMP on the SNMP Properties page on the web-browser interface. When you enable SNMP on the web-browser interface, the access point automatically creates a community string called *public* with read-only access to the IEEE802dot11 MIB.

Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the access point.

Optionally, you can specify one or more of these characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent
- A MIB view, which defines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community

Note In the current Cisco IOS MIB agent implementation, the default community string is for the Internet MIB object sub-tree. Because IEEE802dot11 is under another branch of the MIB object tree, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree. ISO is the common parent node of IEEE (IEEE802dot11) and Internet. This MIB agent behavior is different from the MIB agent behavior on access points not running Cisco IOS software.

Beginning in privileged EXEC mode, follow these steps to configure a community string on the access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server community** *string* [*access-list-number*] [**view** *mib-view*] [**ro** | **rw**]	Configure the community string. • For *string*, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length. • (Optional) For *access-list-number*, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999. • (Optional) For **view** *mib-view*, specify a MIB view to which this community has access, such as **ieee802dot11**. See the "Using the snmp-server view Command" section on page 18-9 for instructions on using the **snmp-server view** command to access Standard IEEE 802.11 MIB objects through IEEE view. • (Optional) Specify either read-only (**ro**) if you want authorized management stations to retrieve MIB objects, or specify read/write (**rw**) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects. **Note** To access the IEEE802dot11 MIB, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	(Optional) If you specified an IP standard access list number in Step 2, then create the list, repeating the command as many times as necessary. • For *access-list-number*, enter the access list number specified in Step 2. • The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched. • For *source*, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent. • (Optional) For *source-wildcard*, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string). To remove a specific community string, use the **no snmp-server community** *string* global configuration command.

This example shows how to assign the strings *open* and *ieee* to SNMP, to allow read-write access for both, and to specify that *open* is the community string for queries on non-IEEE802dot11-MIB objects and *ieee* is the community string for queries on IEEE802dot11-mib objects:

```
ap(config)# snmp-server view dot11view ieee802dot11 included
ap(config)# snmp-server community open rw
ap(config)# snmp-server community ieee view ieee802dot11 rw
```

Configuring Trap Managers and Enabling Traps

A trap manager is a management station that receives and processes traps. Traps are system alerts that the access point generates when certain events occur. By default, no trap manager is defined, and no traps are issued.

Access points running this Cisco IOS release can have an unlimited number of trap managers. Community strings can be any length.

Table 18-3 describes the supported access point traps (notification types). You can enable any or all of these traps and configure a trap manager to receive them.

Table 18-3 Notification Types

Notification Type	Description
authenticate-fail	Enable traps for authentication failures.
config	Enable traps for SNMP configuration changes.
deauthenticate	Enable traps for client device deauthentications.
disassociate	Enable traps for client device disassociations.
dot11-qos	Enable traps for QoS changes.
entity	Enable traps for SNMP entity changes.
rogue-ap	Enable traps for rogue access point detections.
snmp	Enable traps for SNMP events.
switch-over	Enable traps for switch-overs.
syslog	Enable syslog traps.
wlan-wep	Enable WEP traps.

Some notification types cannot be controlled with the **snmp-server enable** global configuration command, such as **tty** and **udp-port**. These notification types are always enabled. You can use the **snmp-server host** global configuration command to a specific host to receive the notification types listed in Table 18-3.

Beginning in privileged EXEC mode, follow these steps to configure the access point to send traps to a host:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c**}} *community-string notification-type*	Specify the recipient of the trap message. • For *host-addr,* specify the name or address of the host (the targeted recipient). • Specify **traps** (the default) to send SNMP traps to the host. Specify **informs** to send SNMP informs to the host. • Specify the SNMP version to support. Version 1, the default, is not available with informs. **Note** Though visible in the command-line help string, the **version 3** keyword (SNMPv3) is not supported. • For *community-string,* specify the string to send with the notification operation. Though you can set this string using the **snmp-server host** command, Cisco recommends that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • For *notification-type*, use the keywords listed in Table 18-3 on page 18-7.
Step 3	**snmp-server enable traps** *notification-types*	Enable the access point to send specific traps. For a list of traps, see Table 18-3 on page 18-7. To enable multiple types of traps, you must issue a separate **snmp-server enable traps** command for each trap type.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the specified host from receiving traps, use the **no snmp-server host** *host* global configuration command. To disable a specific trap type, use the **no snmp-server enable traps** *notification-types* global configuration command.

Setting the Agent Contact and Location Information

Beginning in privileged EXEC mode, follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server contact** *text*	Set the system contact string. For example: `snmp-server contact Dial System Operator at beeper 21555.`
Step 3	**snmp-server location** *text*	Set the system location string. For example: `snmp-server location Building 3/Room 222`
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Using the snmp-server view Command

In global configuration mode, use the **snmp-server view** command to access Standard IEEE 802.11 MIB objects through IEEE view and the dot11 read-write community string.

This example shows how to enable IEEE view and dot11 read-write community string:

```
AP(config)# snmp-server view ieee ieee802dot11 included
AP(config)# snmp-server community dot11 view ieee RW
```

SNMP Examples

This example shows how to enable SNMPv1 and SNMPv2C. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*. This configuration does not cause the access point to send any traps.

```
AP(config)# snmp-server community public
```

This example shows how to assign the strings *open* and *ieee* to SNMP, to allow read-write access for both, and to specify that *open* is the community string for queries on non-IEEE802dot11-MIB objects and *ieee* is the community string for queries on IEEE802dot11-mib objects:

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string *public*. The access point also sends config traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string *public* is sent with the traps.

```
AP(config)# snmp-server community public
AP(config)# snmp-server enable traps config
AP(config)# snmp-server host 192.180.1.27 version 2c public
AP(config)# snmp-server host 192.180.1.111 version 1 public
AP(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the *comaccess* community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host *cisco.com* using the community string *public*.

```
AP(config)# snmp-server community comaccess ro 4
AP(config)# snmp-server enable traps snmp authentication
AP(config)# snmp-server host cisco.com version 2c public
```

This example shows how to send Entity MIB traps to the host *cisco.com*. The community string is restricted. The first line enables the access point to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous **snmp-server host** commands for the host *cisco.com*.

```
AP(config)# snmp-server enable traps entity
AP(config)# snmp-server host cisco.com restricted entity
```

This example shows how to enable the access point to send all traps to the host *myhost.cisco.com* using the community string *public*:

```
AP(config)# snmp-server enable traps
AP(config)# snmp-server host myhost.cisco.com public
```

Displaying SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the **show snmp** privileged EXEC command. For information about the fields in this display, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

CHAPTER 19

Configuring Repeater and Standby Access Points

This chapter descibes how to configure your access point as a hot standby unit or as a repeater unit. This chapter contains these sections:

- Understanding Repeater Access Points, page 19-2
- Configuring a Repeater Access Point, page 19-3
- Understanding Hot Standby, page 19-8
- Configuring a Hot Standby Access Point, page 19-8

Understanding Repeater Access Points

A repeater access point is not connected to the wired LAN; it is placed within radio range of an access point connected to the wired LAN to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. You can configure either the 2.4-GHz radio or the 5-GHz radio as a repeater. In access points with two radios, only one radio can be a repeater; the other radio must be configured as a root radio.

The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. When you configure an access point as a repeater, the access point's Ethernet port does not forward traffic.

You can set up a chain of several repeater access points, but throughput for client devices at the end of the repeater chain will be quite low. Because each repeater must receive and then re-transmit each packet on the same channel, throughput is cut in half for each repeater you add to the chain.

A repeater access point associates to the access point with which it has the best connectivity. However, you can specify the access point to which the repeater associates. Setting up a static, specific association between a repeater and a root access point improves repeater performance.

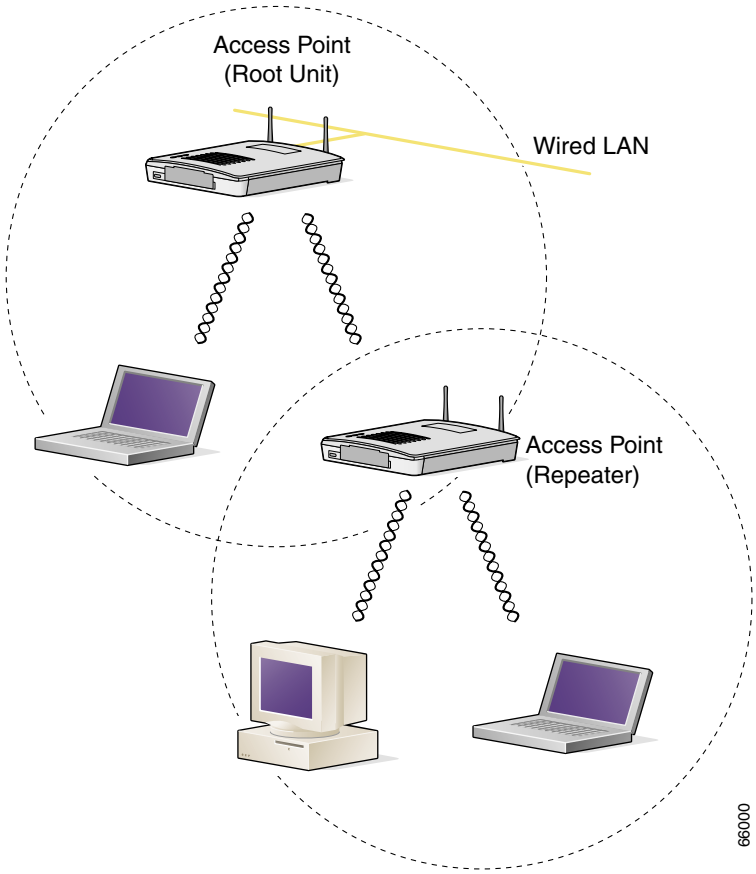
To set up repeaters, you must enable Aironet extensions on both the parent (root) access point and the repeater access points. Aironet extensions, which are enabled by default, improve the access point's ability to understand the capabilities of Cisco Aironet client devices associated with the access point. Disabling Aironet extensions sometimes improves the interoperability between the access point and non-Cisco client devices. Non-Cisco client devices might have difficulty communicating with repeater access points and the root access point to which repeaters are associated.

Note Because access points create a virtual interface for each radio interface, repeater access points associate to the root access point twice: once for the actual interface and once for the virtual interface.

Note You cannot configure multiple VLANs on repeater access points. Repeater access points support only the native VLAN.

Figure 19-1 shows an access point acting as a repeater.

Figure 19-1 Access Point as a Repeater



Configuring a Repeater Access Point

This section provides instructions for setting up an access point as a repeater and includes these sections:

- Default Configuration, page 19-4
- Guidelines for Repeaters, page 19-4
- Setting Up a Repeater, page 19-4
- Verifying Repeater Operation, page 19-5
- Setting Up a Repeater As a LEAP Client, page 19-6
- Setting Up a Repeater As a WPA Client, page 19-7

Default Configuration

Access points are configured as root units by default. Table 19-1 shows the default values for settings that control the access point's role in the wireless LAN.

Table 19-1 Default Settings for Role in Wireless LAN

Feature	Default Setting
Station role	Root
Parent	none
Extensions	Aironet

Guidelines for Repeaters

Follow these guidelines when configuring repeater access points:

- Use repeaters to serve client devices that do not require high throughput. Repeaters extend the coverage area of your wireless LAN, but they drastically reduce throughput.
- Use repeaters when most if not all client devices that associate with the repeaters are Cisco Aironet clients. Non-Cisco client devices sometimes have trouble communicating with repeater access points.
- Make sure that the data rates configured on the repeater access point match the data rates on the parent access point. For instructions on configuring data rates, see the "Configuring Radio Data Rates" section on page 6-4.
- Repeater access points support only the native VLAN. You cannot configure multiple VLANs on a repeater access point.

Note Repeater access points running Cisco IOS software cannot associate to parent access points that that do not run Cisco IOS software.

Note Repeater access points do not support wireless domain services (WDS). Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.

Setting Up a Repeater

Beginning in Privileged Exec mode, follow these steps to configure an access point as a repeater:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	**ssid** *ssid-string*	Create the SSID that the repeater uses to associate to a root access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the root access point, create the same SSID on the repeater, also.
Step 4	**infrastructure-ssid** [**optional**]	Designate the SSID as an infrastructure SSID. The repeater uses this SSID to associate to the root access point. Infrastructure devices must associate to the repeater access point using this SSID unless you also enter the **optional** keyword.
Step 5	**exit**	Exit SSID configuration mode and return to radio interface configuration mode.
Step 6	**station-role repeater**	Set the access point's role in the wireless LAN to repeater.
Step 7	**dot11 extensions aironet**	If Aironet extensions are disabled, enable Aironet extensions.
Step 8	**parent** {*1-4*} *mac-address* [*timeout*]	(Optional) Enter the MAC address for the access point to which the repeater should associate. • You can enter MAC addresses for up to four parent access points. The repeater attempts to associate to MAC address 1 first; if that access point does not respond, the repeater tries the next access point in its parent list. • (Optional) You can also enter a timeout value in seconds that determines how long the repeater attempts to associate to a parent access point before trying the next parent in the list. Enter a timeout value from 0 to 65535 seconds.
Step 9	**end**	Return to privileged EXEC mode.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to set up a repeater acess point with three potential parents:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# exit
AP(config-if)# station-role repeater
AP(config-if)# dot11 extensions aironet
AP(config-if)# parent 1 0987.1234.h345 900
AP(config-if)# parent 2 7809.b123.c345 900
AP(config-if)# parent 3 6543.a456.7421 900
AP(config-if)# end
```

Verifying Repeater Operation

After you set up the repeater, check the LEDs on top of the repeater access point. If your repeater is functioning correctly, the LEDs on the repeater and the root access point to which it is associated behave like this:

- The status LED on the root access point is steady green, indicating that at least one client device is associated with it (in this case, the repeater).

- The status LED on the repeater access point is steady green when it is associated with the root access point and the repeater has client devices associated to it. The repeater's status LED flashes (steady green for 7/8 of a second and off for 1/8 of a second) when it is associated with the root access point but the repeater has no client devices associated to it.

The repeater access point should also appear as associated with the root access point in the root access point's Association Table.

Setting Up a Repeater As a LEAP Client

You can set up a repeater access point to authenticate to your network like other wireless client devices. After you provide a network username and password for the repeater access point, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys.

Setting up a repeater as a LEAP client requires three major steps:

1. Create an authentication username and password for the repeater on your authentication server.
2. Configure LEAP authentication on the root access point to which the repeater associates. The access point to which the repeater associates is called the parent access point. See Chapter 10, "Configuring Authentication Types," for instructions on setting up authentication.

Note On the repeater access point, you must enable the same cipher suite or WEP encryption method and WEP features that are enabled on the parent access point.

3. Configure the repeater to act as a LEAP client. Beginning in Privileged Exec mode, follow these instructions to set up the repeater as a LEAP client:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters, but they should not include spaces. SSIDs are case-sensitive.
Step 4	**authentication network-eap** *list-name*	Enable LEAP authentication on the repeater so that LEAP-enabled client devices can authenticate through the repeater. For list-name, specify the list name you want to use for EAP authentication. You define list names for EAP and for MAC addresses using the **aaa authentication login** command. These lists define the authentication methods activated when a user logs in and indirectly identify the location where the authentication information is stored.
Step 5	**authentication client username** *username* **password** *password*	Configure the username and password that the repeater uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the repeater on the authentication server.

	Command	Purpose
Step 6	**infrastructure ssid** [**optional**]	(Optional) Designate the SSID as the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. If you designate an SSID as the infrastructure SSID, infrastructure devices must associate to the access point using that SSID unless you also enter the **optional** keyword.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Setting Up a Repeater As a WPA Client

WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. You can set up a repeater access point to authenticate to your network like other WPA-enabled client devices.

Beginning in Privileged Exec mode, follow these steps to set up the repeater as a WPA client:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.
Step 4	**authentication open**	Enable open authentication for the SSID.
Step 5	**authentication key-management wpa**	Enable WPA authenticated key management for the SSID.
Step 6	**infrastructure ssid**	Designate the SSID as the SSID that the repeater uses to associate to other access points.
Step 7	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	Enter a pre-shared key for the repeater. Enter the key using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter from 8 to 63 ASCII characters, and the access point expands the key for you.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Understanding Hot Standby

Hot Standby mode designates an access point as a backup for another access point. The standby access point is placed near the access point it monitors, configured exactly the same as the monitored access point. The standby access point associates with the monitored access point as a client and sends IAPP queries to the monitored access point through both the Ethernet and the radio ports. If the monitored access point fails to respond, the standby access point comes online and takes the monitored access point's place in the network.

Except for the IP address, the standby access point's settings should be identical to the settings on the monitored access point. If the monitored access point goes offline and the standby access point takes its place in the network, matching settings ensures that client devices can switch easily to the standby access point.

The standby access point monitors another access point in a device-to-device relationship, not in an interface-to-interface relationship. For example, you cannot configure the standby access point's 5-GHz radio to monitor the 5-GHz radio in access point alpha and the standby's 2.4-GHz radio to monitor the 2.4-GHz radio in access point bravo. You also cannot configure one radio in a dual-radio access point as a standby radio and configure the other radio to serve client devices.

Hot standby mode is disabled by default.

Note If the monitored access point malfunctions and the standby access point takes its place, repeat the hot standby setup on the standby access point when you repair or replace the monitored access point. The standby access point does not revert to standby mode automatically.

Configuring a Hot Standby Access Point

When you set up the standby access point, you must enter the MAC address of the access point that the standby unit will monitor. Record the MAC address of the monitored access point before you configure the standby access point.

The standby access point also must duplicate several key settings on the monitored access point. These settings are:

- Primary SSID (as well as additional SSIDs configured on the monitored access point)
- Default IP Subnet Mask
- Default Gateway
- Data rates
- WEP settings
- Authentication types and authentication servers

Check the monitored access point and record these settings before you set up the standby access point.

Note Wireless client devices associated to the standby access point lose their connections during the hot standby setup process.

Tip To quickly duplicate the monitored access point's settings on the standby access point, save the monitored access point configuration and load it on the standby access point. See the "Working with Configuration Files" section on page 20-8 for instructions on uploading and downloading configuration files.

Beginning in Privileged Exec mode, follow these steps to enable hot standby mode on an access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**iapp standby** *mac-address*	Puts the access point into standby mode and specifies the MAC address of radio on the monitored access point. **Note** When you configure a 1200 Series access point with two radios to monitor a 1200 Series access point with two radios, you must enter the MAC addresses of both the monitored 2.4-GHz and 5-GHz radios. Enter the 2.4-GHz radio MAC address first, followed by the 5-GHz radio MAC address.
Step 3	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 4	**ssid** *ssid-string*	Create the SSID that the standby access point uses to associate to the monitored access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the monitored access point, create the same SSID on the standby access point, also.
Step 5	**infrastructure-ssid** [**optional**]	Designate the SSID as an infrastructure SSID. The standby uses this SSID to associate to the monitored access point. If the standby access point takes the place of the monitored access point, infrastructure devices must associate to the standby access point using this SSID unless you also enter the **optional** keyword.
Step 6	**authentication client username** *username* **password** *password*	If the monitored access point is configured to require LEAP authentication, configure the username and password that the standby access point uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the standby access point on the authentication server.
Step 7	**exit**	Exit SSID configuration mode and return to radio interface configuration mode.
Step 8	**iapp standby poll-frequency** *seconds*	Sets the number of seconds between queries that the standby access point sends to the monitored access point's radio and Ethernet ports. The default poll frequency is 2 seconds.
Step 9	**iapp standby timeout** *seconds*	Sets the number of seconds the standby access point waits for a response from the monitored access point before it assumes that the monitored access point has malfunctioned. The default timeout is 20 seconds.

	Command	Purpose
Step 10	**iapp standby primary-shutdown**	(Optional) Configures the standby access point to send a Dumb Device Protocol (DDP) message to the monitored access point to disable the radios of the monitored access point when the standby unit becomes active. This feature prevents client devices that are associated to the monitored access point from remaining associated to the malfunctioning unit.
Step 11	**show iapp standby-parms**	Verify your entries. If the access point is in standby mode, this command displays the standby parameters, including the MAC address of the monitored access point and the poll-frequency and timeout values. If the access point is not in standby mode, *no iapp standby mac-address* appears.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

After you enable standby mode, configure the settings that you recorded from the monitored access point to match on the standby access point.

Verifying Standby Operation

Use this command to check the status of the standby access point:

show iapp standby-status

This command displays the status of the standby access point. Table 19-2 lists the standby status messages that can appear.

Table 19-2 Standby Status Messages

Message	Description
IAPP Standby is Disabled	The access point is not configured for standby mode.
IAPP—AP is in standby mode	The access point is in standby mode.
IAPP—AP is operating in active mode	The standby access point has taken over for the monitored access point and is functioning as a root access point.
IAPP—AP is operating in repeater mode	The standby access point has taken over for the monitored access point and is functioning as a repeater access point.
Standby status: Initializing	The standby access point is initializing link tests with the monitored access point.
Standby status: Takeover	The standby access point has transitioned to active mode.
Standby status: Stopped	Standby mode has been stopped by a configuration command.
Standby status: Ethernet Linktest Failed	An Ethernet link test failed from the standby access point to the monitored access point.
Standby status: Radio Linktest Failed	A radio link test failed from the standby access point to the monitored access point.
Standby status: Standby Error	An undefined error occurred.

Table 19-2 Standby Status Messages (continued)

Message	Description
Standby State: Init	The standby access point is initializing link tests with the monitored access point.
Standby State: Running	The standby access point is operating in standby mode and is running link tests to the monitored access point.
Standby State: Stopped	Standby mode has been stopped by a configuration command.
Standby State: Not Running	The access point is not in standby mode.

Use this command to check the standby configuration:

show iapp standby-parms

This command displays the MAC address of the standby access point, the standby timeout, and the poll-frequency values. If no standby access point is configured, this message appears:

```
no iapp standby mac-address
```

If a standby access point takes over for the monitored access point, you can use the **show iapp statistics** command to help determine the reason that the standby access point took over.

CHAPTER 20

Managing Firmware and Configurations

This chapter describes how to manipulate the Flash file system, how to copy configuration files, and how to archive (upload and download) software images.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco Aironet 1200 Series Access Point Command Reference* for this release and the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This chapter consists of these sections:

- Working with the Flash File System, page 20-2
- Working with Configuration Files, page 20-8
- Working with Software Images, page 20-18

Working with the Flash File System

The Flash file system on your access point provides several commands to help you manage software image and configuration files.

The Flash file system is a single Flash device on which you can store files. This Flash device is called *flash:*.

This section contains this information:

- Displaying Available File Systems, page 20-2
- Setting the Default File System, page 20-3
- Displaying Information About Files on a File System, page 20-3
- Changing Directories and Displaying the Working Directory, page 20-4
- Creating and Removing Directories, page 20-4
- Copying Files, page 20-5
- Deleting Files, page 20-5
- Creating, Displaying, and Extracting tar Files, page 20-6
- Displaying the Contents of a File, page 20-8

Displaying Available File Systems

To display the available file systems on your access point, use the **show file systems** privileged EXEC command as shown in this example:

```
ap# show file systems
File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
*   16128000    11118592     flash     rw   flash:
    16128000    11118592   unknown     rw   zflash:
       32768       26363     nvram     rw   nvram:
           -           -   network     rw   tftp:
           -           -    opaque     rw   null:
           -           -    opaque     rw   system:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
```

Table 20-1 lists field descriptions for the **show file systems** command.

Table 20-1 show file systems Field Descriptions

Field	Value
Size(b)	Amount of memory in the file system in bytes.
Free(b)	Amount of free memory in the file system in bytes.

Table 20-1 show file systems Field Descriptions (continued)

Field	Value
Type	Type of file system. **flash**—The file system is for a Flash memory device. **network**—The file system is for a network device. **nvram**—The file system is for a nonvolatile RAM (NVRAM) device. **opaque**—The file system is a locally generated *pseudo* file system (for example, the *system*) or a download interface, such as brimux. **unknown**—The file system is an unknown type.
Flags	Permission for file system. **ro**—read-only. **rw**—read/write. **wo**—write-only.
Prefixes	Alias for file system. **flash:**—Flash file system. **ftp:**—File Transfer Protocol network server. Used to transfer files to or from the network device. **nvram:**—Non-volatile RAM memory (NVRAM). **null:**—Null destination for copies. You can copy a remote file to null to determine its size. **rcp:**—Remote Copy Protocol (RCP) network server. **system:**—Contains the system memory, including the running configuration. **tftp:**—Trivial File Transfer Protocol (TFTP) network server. **zflash:**—Read-only file decompression file system, which mirrors the contents of the Flash file system.

Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the **cd** *filesystem:* privileged EXEC command. You can set the default file system to omit the *filesystem:* argument from related commands. For example, for all privileged EXEC commands that have the optional *filesystem:* argument, the system uses the file system specified by the **cd** command.

By default, the default file system is *flash:*.

You can display the current default file system as specified by the **cd** command by using the **pwd** privileged EXEC command.

Displaying Information About Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to Flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a Flash configuration file to another location, you might want to verify its filename for use in another command.

To display information about files on a file system, use one of the privileged EXEC commands in Table 20-2:

Table 20-2 Commands for Displaying Information About Files

Command	Description
dir [**/all**] [*filesystem***:**][*filename*]	Display a list of files on a file system.
show file systems	Display more information about each of the files on a file system.
show file information *file-url*	Display information about a specific file.
show file descriptors	Display a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.

Changing Directories and Displaying the Working Directory

Beginning in privileged EXEC mode, follow these steps to change directories and display the working directory.

	Command	Purpose
Step 1	**dir** *filesystem***:**	Display the directories on the specified file system. For *filesystem***:**, use **flash:** for the system board Flash device.
Step 2	**cd new_configs**	Change to the directory of interest. The command example shows how to change to the directory named *new_configs*.
Step 3	**pwd**	Display the working directory.

Creating and Removing Directories

Beginning in privileged EXEC mode, follow these steps to create and remove a directory:

	Command	Purpose
Step 1	**dir** *filesystem***:**	Display the directories on the specified file system. For *filesystem***:**, use **flash:** for the system board Flash device.
Step 2	**mkdir old_configs**	Create a new directory. The command example shows how to create the directory named *old_configs*. Directory names are case sensitive. Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.
Step 3	**dir** *filesystem***:**	Verify your entry.

To delete a directory with all its files and subdirectories, use the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command.

Use the **/recursive** keyword to delete the named directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the name of the directory to be deleted. All the files in the directory and the directory are removed.

Caution When files and directories are deleted, their contents cannot be recovered.

Copying Files

To copy a file from a source to a destination, use the **copy** [**/erase**] *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of Flash memory to be used as the configuration during system initialization.

Network file system URLs include **ftp:**, **rcp:**, and **tftp:** and have the following syntax:

- File Transfer Protocol (FTP)—**ftp:**[[**//***username* [**:***password*]**@***location*]**/***directory*]**/***filename*
- Remote Copy Protocol (RCP)—**rcp:**[[**//***username***@***location*]**/***directory*]**/***filename*
- Trivial File Transfer Protocol (TFTP)—**tftp:**[[**//***location*]**/***directory*]**/***filename*

Local writable file systems include flash:.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

For specific examples of using the **copy** command with configuration files, see the "Working with Configuration Files" section on page 20-8.

To copy software images either by downloading a new version or uploading the existing one, use the **archive download-sw** or the **archive upload-sw** privileged EXEC command. For more information, see the "Working with Software Images" section on page 20-18.

Deleting Files

When you no longer need a file on a Flash memory device, you can permanently delete it. To delete a file or directory from a specified Flash device, use the **delete** [**/force**] [**/recursive**] [*filesystem***:**]*file-url* privileged EXEC command.

Caution When files are deleted, their contents cannot be recovered.

Use the **/recursive** keyword for deleting a directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

If you omit the *filesystem***:** option, the access point uses the default device specified by the **cd** command. For *file-url*, you specify the path (directory) and the name of the file to be deleted.

This example shows how to delete the file *myconfig* from the default Flash memory device:

```
ap# delete myconfig
```

Creating, Displaying, and Extracting tar Files

You can create a tar file and write files into it, list the files in a tar file, and extract the files from a tar file as described in the next sections.

Creating a tar File

To create a tar file and write files into it, use this privileged EXEC command:

archive tar /create *destination-url* **flash:/***file-url*

For *destination-url*, specify the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:

- For the local Flash file system, the syntax is **flash:/***file-url*
- For the File Transfer Protocol (FTP), the syntax is **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**

The *tar-filename***.tar** is the tar file to be created.

For **flash:/***file-url*, specify the location on the local Flash file system from which the new tar file is created. You can also specify an optional list of files or directories within the source directory to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.

This example shows how to create a tar file. This command writes the contents of the *new-configs* directory on the local Flash device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
ap# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

Displaying the Contents of a tar File

To display the contents of a tar file on the screen, use this privileged EXEC command:

archive tar /table *source-url*

For *source-url*, specify the source URL alias for the local or network file system. These options are supported:

- For the local Flash file system, the syntax is **flash:**
- For the File Transfer Protocol (FTP), the syntax is **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**

The *tar-filename***.tar** is the tar file to display.

You can also limit the display of the files by specifying an optional list of files or directories after the tar file; then only these files are displayed. If none are specified, all files and directories are displayed.

This example shows how to display the contents of the *c1200-k9w7-mx.122-8.JA.tar* file that is in Flash memory:

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA.tar
info (219 bytes)
c1200-k9w7-mx.122-8.JA/ (directory)
c1200-k9w7-mx.122-8.JA/html/ (directory)
c1200-k9w7-mx.122-8.JA/html/foo.html (0 bytes)
c1200-k9w7-mx.122-8.JA/c1200-k9w7-mx.122-8.JA.bin (610856 bytes)
c1200-k9w7-mx.122-8.JA/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *c1200-k9w7-mx.122-8.JA/html* directory and its contents:

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA/html
c1200-k9w7-mx.122-8.JA/html/ (directory)
c1200-k9w7-mx.122-8.JA/html/foo.html (0 bytes)
```

Extracting a tar File

To extract a tar file into a directory on the Flash file system, use this privileged EXEC command:

archive tar /xtract *source-url* **flash:/***file-url*

For *source-url*, specify the source URL alias for the local or network file system. These options are supported:

- For the local Flash file system, the syntax is **flash:**
- For the File Transfer Protocol (FTP), the syntax is **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**

The *tar-filename***.tar** is the tar file from which to extract files.

For **flash:/***file-url*, specify the location on the local Flash file system into which the tar file is extracted. You can also specify an optional list of files or directories within the tar file for extraction. If none are specified, all files and directories are extracted.

This example shows how to extract the contents of a tar file located on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local Flash file system. The remaining files in the *saved.tar* file are ignored.

```
ap# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

Displaying the Contents of a File

To display the contents of any readable file, including a file on a remote file system, use the **more** [**/ascii** | **/binary** | **/ebcdic**] *file-url* privileged EXEC command:

This example shows how to display the contents of a configuration file on a TFTP server:

```
ap# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!

<output truncated>
```

Working with Configuration Files

This section describes how to create, load, and maintain configuration files. Configuration files contain commands entered to customize the function of the Cisco IOS software. To better benefit from these instructions, your access point contains a minimal default running configuration for interacting with the system software.

You can copy (*download*) configuration files from a TFTP, FTP, or RCP server to the running configuration of the access point for various reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another access point. For example, you might add another access point to your network and want it to have a configuration similar to the original access point. By copying the file to the new access point, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on all the access points in your network so that all the access points have similar configurations.

You can copy (*upload*) configuration files from the access point to a file server by using TFTP, FTP, or RCP. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection oriented.

This section includes this information:

- Guidelines for Creating and Using Configuration Files, page 20-9
- Configuration File Types and Location, page 20-9
- Creating a Configuration File by Using a Text Editor, page 20-10
- Copying Configuration Files by Using TFTP, page 20-10
- Copying Configuration Files by Using FTP, page 20-12
- Copying Configuration Files by Using RCP, page 20-15
- Clearing Configuration Information, page 20-18

Guidelines for Creating and Using Configuration Files

Creating configuration files can aid in your access point configuration. Configuration files can contain some or all of the commands needed to configure one or more access points. For example, you might want to download the same configuration file to several access points that have the same hardware configuration.

Use these guidelines when creating a configuration file:

- If no passwords have been set on the access point, you must set them on each access point by entering the **enable secret** *secret-password* global configuration command. Enter a blank line for this command. The password is saved in the configuration file as clear text.
- If passwords already exist, you cannot enter the **enable secret** *secret-password* global configuration command in the file because the password verification will fail. If you enter a password in the configuration file, the access point mistakenly attempts to execute the passwords as commands as it executes the file.
- The **copy** {**ftp: | rcp: | tftp:**} **system:running-config** privileged EXEC command loads the configuration files on the access point as if you were entering the commands at the command line. The access point does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is erased. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration might not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

  To restore a configuration file to an exact copy of a file stored on a server, copy the configuration file directly to the startup configuration (by using the **copy** {**ftp: | rcp: | tftp:**} **nvram:startup-config** privileged EXEC command), and reload the access point.

Configuration File Types and Location

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the **copy running-config startup-config** privileged EXEC command.

The running configuration is saved in DRAM; the startup configuration is stored in the NVRAM section of Flash memory.

Creating a Configuration File by Using a Text Editor

When creating a configuration file, you must list commands logically so that the system can respond appropriately. This is one method of creating a configuration file:

Step 1 Copy an existing configuration from an access point to a server.

For more information, see the "Downloading the Configuration File by Using TFTP" section on page 20-11, the "Downloading a Configuration File by Using FTP" section on page 20-13, or the "Downloading a Configuration File by Using RCP" section on page 20-16.

Step 2 Open the configuration file in a text editor such as vi or emacs on UNIX or Notepad on a PC.

Step 3 Extract the portion of the configuration file with the desired commands, and save it in a new file.

Step 4 Copy the configuration file to the appropriate server location. For example, copy the file to the TFTP directory on the workstation (usually /tftpboot on a UNIX workstation).

Step 5 Make sure the permissions on the file are set to world-read.

Copying Configuration Files by Using TFTP

You can configure the access point by using configuration files you create, download from another access point, or download from a TFTP server. You can copy (upload) configuration files to a TFTP server for storage.

This section includes this information:

- Preparing to Download or Upload a Configuration File by Using TFTP, page 20-10
- Downloading the Configuration File by Using TFTP, page 20-11
- Uploading the Configuration File by Using TFTP, page 20-11

Preparing to Download or Upload a Configuration File by Using TFTP

Before you begin downloading or uploading a configuration file by using TFTP, perform these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the /etc/services file contains this line:

  ```
  tftp 69/udp
  ```

  Note You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, refer to the documentation for your workstation.

- Ensure that the access point has a route to the TFTP server. The access point and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.

- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server (usually */*tftpboot on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch** *filename* command, where *filename* is the name of the file you will use when uploading it to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading the Configuration File by Using TFTP

To configure the access point by using a configuration file downloaded from a TFTP server, follow these steps:

Step 1 Copy the configuration file to the appropriate TFTP directory on the workstation.

Step 2 Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using TFTP" section on page 20-10.

Step 3 Log into the access point through a Telnet session.

Step 4 Download the configuration file from the TFTP server to configure the access point.

Specify the IP address or host name of the TFTP server and the name of the file to download.

Use one of these privileged EXEC commands:

- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **system:running-config**
- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **nvram:startup-config**

The configuration file downloads, and the commands are executed as the file is parsed line-by-line.

This example shows how to configure the software from the file *tokyo-confg* at IP address 172.16.2.155:

```
ap# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

Uploading the Configuration File by Using TFTP

To upload a configuration file from an access point to a TFTP server for storage, follow these steps:

Step 1 Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using TFTP" section on page 20-10.

Step 2 Log into the access point through a Telnet session.

Step 3 Upload the access point configuration to the TFTP server. Specify the IP address or host name of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

- **copy system:running-config tftp:**[[[*//location*]*/directory*]*/filename*]
- **copy nvram:startup-config tftp:**[[[*//location*]*/directory*]*/filename*]

The file is uploaded to the TFTP server.

This example shows how to upload a configuration file from an access point to a TFTP server:

```
ap# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!! [OK]
```

Copying Configuration Files by Using FTP

You can copy configuration files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the access point to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The access point sends the first valid password in this list:

- The password specified in the **copy** command if a password is specified.
- The password set by the **ip ftp password** *password* global configuration command if the command is configured.
- The access point forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, *apname* is the configured host name, and *domain* is the domain of the access point.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept your FTP write request.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify only a username for that copy operation.

If the server has a directory structure, the configuration file is written to or copied from the directory associated with the username on the server. For example, if the configuration file resides in the home directory of a user on the server, specify that user's name as the remote username.

For more information, refer to the documentation for your FTP server.

This section includes this information:

- Preparing to Download or Upload a Configuration File by Using FTP, page 20-13
- Downloading a Configuration File by Using FTP, page 20-13
- Uploading a Configuration File by Using FTP, page 20-14

Preparing to Download or Upload a Configuration File by Using FTP

Before you begin downloading or uploading a configuration file by using FTP, perform these tasks:

- Ensure that the access point has a route to the FTP server. The access point and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the **ping** command.
- If you are accessing the access point through a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command during all copy operations. The new username is stored in NVRAM. If you are accessing the access point through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a configuration file to the FTP server, it must be properly configured to accept the write request from the user on the access point.

For more information, refer to the documentation for your FTP server.

Downloading a Configuration File by Using FTP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using FTP:

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using FTP" section on page 20-13.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode on the access point. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*] **system:running-config** or **copy ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*] **nvram:startup-config**	Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

This example shows how to copy a configuration file named *host1-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the access point:

```
ap# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
```

```
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. The software copies the configuration file *host2-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the access point startup configuration.

```
ap# configure terminal
ap(config)# ip ftp username netadmin1
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

Uploading a Configuration File by Using FTP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using FTP:

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using FTP" section on page 20-13.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy system:running-config ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*] or **copy nvram:startup-config ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*]	Using FTP, store the access point running or startup configuration file to the specified location.

This example shows how to copy the running configuration file named *ap2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
ap# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/ap2-confg
Write file ap2-confg on host 172.16.101.101?[confirm]
```

```
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

This example shows how to store a startup configuration file on a server by using FTP to copy the file:

```
ap# configure terminal
ap(config)# ip ftp username netadmin2
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101?[confirm]
![OK]
```

Copying Configuration Files by Using RCP

The Remote Copy Protocol (RCP) provides another method of downloading, uploading, and copying configuration files between remote hosts and the access point. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

The RCP requires a client to send a remote username with each RCP request to a server. When you copy a configuration file from the access point to a server, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is configured.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the access point software sends the Telnet username as the remote username.
- The access point host name.

For a successful RCP copy request, you must define an account on the network server for the remote username. If the server has a directory structure, the configuration file is written to or copied from the directory associated with the remote username on the server. For example, if the configuration file is in the home directory of a user on the server, specify that user's name as the remote username.

This section includes this information:

- Preparing to Download or Upload a Configuration File by Using RCP, page 20-16
- Downloading a Configuration File by Using RCP, page 20-16
- Uploading a Configuration File by Using RCP, page 20-17

Preparing to Download or Upload a Configuration File by Using RCP

Before you begin downloading or uploading a configuration file by using RCP, perform these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the access point has a route to the RCP server. The access point and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the access point through a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all copy operations. The new username is stored in NVRAM. If you are accessing the access point through a Telnet session and you have a valid username, this username is used, and you do not need to set the RCP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a file to the RCP server, it must be properly configured to accept the RCP write request from the user on the access point. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose that the access point contains these configuration lines:

  ```
  hostname ap1
  ip rcmd remote-username User0
  ```

  If the access point IP address translates to *ap1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

  ```
  ap1.company.com ap1
  ```

For more information, refer to the documentation for your RCP server.

Downloading a Configuration File by Using RCP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using RCP:

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using RCP" section on page 20-16.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.

	Command	Purpose
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy rcp:**[[[**//**[*username*@]*location*]*/directory*]*/filename*] **system:running-config** or **copy rcp:**[[[**//**[*username*@]*location*]*/directory*]*/filename*] **nvram:startup-config**	Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

This example shows how to copy a configuration file named *host1-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and load and run those commands on the access point:

```
ap# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. Then it copies the configuration file *host2-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin1
ap(config)# end
ap# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

Uploading a Configuration File by Using RCP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using RCP:

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using RCP" section on page 20-16.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.

	Command	Purpose
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy system:running-config rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***filename*] or **copy nvram:startup-config rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***filename*]	Using RCP, copy the configuration file from an access point running or startup configuration file to a network server.

This example shows how to copy the running configuration file named *ap2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
ap# copy system:running-config rcp://netadmin1@172.16.101.101/ap2-confg
Write file ap-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

This example shows how to store a startup configuration file on a server:

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin2
ap(config)# end
ap# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101?[confirm]
![OK]
```

Clearing Configuration Information

This section describes how to clear configuration information.

Deleting a Stored Configuration File

Caution You cannot restore a file after it has been deleted.

To delete a saved configuration from Flash memory, use the **delete flash:***filename* privileged EXEC command. Depending on the setting of the **file prompt** global configuration command, you might be prompted for confirmation before you delete a file. By default, the access point prompts for confirmation on destructive file operations. For more information about the **file prompt** command, refer to the *Cisco IOS Command Reference for Release 12.1*.

Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software, Cisco IOS software, radio firmware, and the web management HTML files.

You download an access point image file from a TFTP, FTP, or RCP server to upgrade the access point software. You upload an access point image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same access point or another of the same type.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection-oriented.

This section includes this information:

- Image Location on the Access Point, page 20-19
- tar File Format of Images on a Server or Cisco.com, page 20-19
- Copying Image Files by Using TFTP, page 20-20
- Copying Image Files by Using FTP, page 20-23
- Copying Image Files by Using RCP, page 20-27
- Reloading the Image Using the Web Browser Interface, page 20-32

Note For a list of software images and supported upgrade paths, refer to the release notes for your access point.

Image Location on the Access Point

The Cisco IOS image is stored in a directory that shows the version number. A subdirectory contains the HTML files needed for web management. The image is stored on the system board Flash memory (flash:).

You can use the **show version** privileged EXEC command to see the software version that is currently running on your access point. In the display, check the line that begins with `System image file is...` It shows the directory name in Flash memory where the image is stored.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images you might have stored in Flash memory.

tar File Format of Images on a Server or Cisco.com

Software images located on a server or downloaded from Cisco.com are provided in a tar file format, which contains these files:

- *info* file

  The info file is always at the beginning of the tar file and contains information about the files within it.
- Cisco IOS image
- Web management files needed by the HTTP server on the access point
- radio firmware 5000.img file
- *info.ver* file

  The info.ver file is always at the end of the tar file and contains the same information as the info file. Because it is the last file in the tar file, its existence means that all files in the image have been downloaded.

Note The tar file sometimes ends with an extension other than *.tar*.

Copying Image Files by Using TFTP

You can download an access point image from a TFTP server or upload the image from the access point to a TFTP server.

You download an access point image file from a server to upgrade the access point software. You can overwrite the current image with the new one.

You upload an access point image file to a server for backup purposes; this uploaded image can be used for future downloads to the same or another access point of the same type.

This section includes this information:

- Preparing to Download or Upload an Image File by Using TFTP, page 20-20
- Downloading an Image File by Using TFTP, page 20-21
- Uploading an Image File by Using TFTP, page 20-22

Preparing to Download or Upload an Image File by Using TFTP

Before you begin downloading or uploading an image file by using TFTP, perform these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the /etc/services file contains this line:

  ```
  tftp 69/udp
  ```

  Note You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, refer to the documentation for your workstation.

- Ensure that the access point has a route to the TFTP server. The access point and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the image to be downloaded is in the correct directory on the TFTP server (usually /tftpboot on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the image file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch** *filename* command, where *filename* is the name of the file you will use when uploading the image to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading an Image File by Using TFTP

You can download a new image file and replace the current image or keep the current image.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow Steps 1 through 3 to download a new image from a TFTP server and overwrite the existing image.

	Command	Purpose
Step 1	.	Copy the image to the appropriate TFTP directory on the workstation. Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File by Using TFTP" section on page 20-20
Step 2		Log into the access point through a Telnet session.
Step 3	**archive download-sw /overwrite /reload tftp:**[[*//location*]*/directory*]*/image-name*	Download the image file from the TFTP server to the access point, and overwrite the current image. • The **/overwrite** option overwrites the software image in Flash with the downloaded image. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For **//***location*, specify the IP address of the TFTP server. • For */directory/image-name*, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 4	**archive download-sw /leave-old-sw /reload tftp:**[[*//location*]*/directory*]*/image-name*	Download the image file from the TFTP server to the access point, and keep the current image. • The **/leave-old-sw** option keeps the old software version after a download. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For **//***location*, specify the IP address of the TFTP server. • For */directory/image-name*, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

Note To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the Flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

Note If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image on the system board Flash device (flash:). The image is placed into a new directory named with the software version string, and the system boot path variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the directory name of the old image. All the files in the directory and the directory are removed.

Uploading an Image File by Using TFTP

You can upload an image from the access point to a TFTP server. You can later download this image to the access point or to another access point of the same type.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow these steps to upload an image to a TFTP server:

	Command	Purpose
Step 1		Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File by Using TFTP" section on page 20-20.
Step 1		Log into the access point through a Telnet session.
Step 2	**archive upload-sw tftp:**[[*//location*]*/directory*]*/image-name***.tar**	Upload the currently running access point image to the TFTP server. • For ***//location***, specify the IP address of the TFTP server. • For */directory/image-name***.tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name***.tar** is the name of the software image to be stored on the server.

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Copying Image Files by Using FTP

You can download an access point image from an FTP server or upload the image from the access point to an FTP server.

You download an access point image file from a server to upgrade the access point software. You can overwrite the current image with the new one or keep the current image after a download.

You upload an access point image file to a server for backup purposes. You can use this uploaded image for future downloads to the access point or another access point of the same type.

This section includes this information:

- Preparing to Download or Upload an Image File by Using FTP, page 20-23
- Downloading an Image File by Using FTP, page 20-24
- Uploading an Image File by Using FTP, page 20-26

Preparing to Download or Upload an Image File by Using FTP

You can copy images files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy an image file from the access point to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The access point sends the first valid password in this list:

- The password specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a password is specified.
- The password set by the **ip ftp password** *password* global configuration command if the command is configured.
- The access point forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, ap*name* is the configured host name, and *domain* is the domain of the access point.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from you.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.

If the server has a directory structure, the image file is written to or copied from the directory associated with the username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using FTP, perform these tasks:

- Ensure that the access point has a route to the FTP server. The access point and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Verify connectivity to the FTP server by using the **ping** command.

- If you are accessing the access point through a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command. This new name will be used during all archive operations. The new username is stored in NVRAM. If you are accessing the access point through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username for that operation only.
- When you upload an image file to the FTP server, it must be properly configured to accept the write request from the user on the access point.

For more information, refer to the documentation for your FTP server.

Downloading an Image File by Using FTP

You can download a new image file and overwrite the current image or keep the current image.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow Steps 1 through 7 to download a new image from an FTP server and overwrite the existing image. To keep the current image, skip Step 7.

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-23.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.
Step 6	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 7	**archive download-sw /overwrite /reload ftp:**[[*//username*[**:***password*]*@location*]*/directory*] */image-name***.tar**	Download the image file from the FTP server to the access point, and overwrite the current image. • The **/overwrite** option overwrites the software image in Flash with the downloaded image. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For ***//username***[**:***password*], specify the username and password; these must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-23. • For *@location*, specify the IP address of the FTP server. • For *directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 8	**archive download-sw /leave-old-sw /reload ftp:**[[*//username*[**:***password*]*@location*]*/directory*] */image-name***.tar**	Download the image file from the FTP server to the access point, and keep the current image. • The **/leave-old-sw** option keeps the old software version after a download. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For ***//username***[**:***password*], specify the username and password. These must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-23. • For *@location*, specify the IP address of the FTP server. • For *directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

Note To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the Flash device, whether or not it is the same as the new one, downloads the new image, and then reloads the software.

Note If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board Flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT path-list is updated to point to the newly installed image. Use the privileged EXEC mode **show boot** command to display boot attributes, and use the global configuration **boot** command to change the boot attributes.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Uploading an Image File by Using FTP

You can upload an image from the access point to an FTP server. You can later download this image to the same access point or to another access point of the same type.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

The upload feature is available only if the HTML pages associated with the Cluster Management Suite (CMS) have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an FTP server:

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using FTP" section on page 20-13.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**archive upload-sw ftp:**[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*]**/***image-name*.**tar**	Upload the currently running access point image to the FTP server. • For **//***username***:***password*, specify the username and password. These must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-23. • For **@***location*, specify the IP address of the FTP server. • For **/***directory***/***image-name*.**tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name*.**tar** is the name of the software image to be stored on the server.

The **archive upload-sw** command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Copying Image Files by Using RCP

You can download an access point image from an RCP server or upload the image from the access point to an RCP server.

You download an access point image file from a server to upgrade the access point software. You can overwrite the current image with the new one or keep the current image after a download.

You upload an access point image file to a server for backup purposes. You can use this uploaded image for future downloads to the same access point or another of the same type.

This section includes this information:

- Preparing to Download or Upload an Image File by Using RCP, page 20-27
- Downloading an Image File by Using RCP, page 20-29
- Uploading an Image File by Using RCP, page 20-31

Preparing to Download or Upload an Image File by Using RCP

RCP provides another method of downloading and uploading image files between remote hosts and the access point. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the access point to a server by using RCP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is entered.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the access point software sends the Telnet username as the remote username.
- The access point host name.

For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. If the server has a directory structure, the image file is written to or copied from the directory associated with the remote username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the access point has a route to the RCP server. The access point and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the access point through a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all archive operations. The new username is stored in NVRAM. If you are accessing the access point through a Telnet session and you have a valid username, this username is used, and there is no need to set the RCP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.
- When you upload an image to the RCP to the server, it must be properly configured to accept the RCP write request from the user on the access point. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose the access point contains these configuration lines:

  ```
  hostname ap1
  ip rcmd remote-username User0
  ```

  If the access point IP address translates to *ap1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

  ```
  ap1.company.com ap1
  ```

For more information, refer to the documentation for your RCP server.

Downloading an Image File by Using RCP

You can download a new image file and replace or keep the current image.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow Steps 1 through 6 to download a new image from an RCP server and overwrite the existing image. To keep the current image, skip Step 6.

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-27.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.
Step 5	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 6	**archive download-sw /overwrite /reload rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***image-name***.tar**]	Download the image file from the RCP server to the access point, and overwrite the current image. • The **/overwrite** option overwrites the software image in Flash with the downloaded image. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For **//***username*, specify the username. For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-27. • For @*location*, specify the IP address of the RCP server. • For **/***directory***/***image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 7	**archive download-sw /leave-old-sw /reload rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***image-name***.tar**]	Download the image file from the RCP server to the access point, and keep the current image. • The **/leave-old-sw** option keeps the old software version after a download. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For **//***username*, specify the username. For the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-27. • For @*location*, specify the IP address of the RCP server. • For **/***directory*]**/***image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

Note To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the Flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

Note If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough room to install the new image an keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board Flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old software during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Uploading an Image File by Using RCP

You can upload an image from the access point to an RCP server. You can later download this image to the same access point or to another access point of the same type.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

The upload feature is available only if the HTML pages associated with the Cluster Management Suite (CMS) have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an RCP server:

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-27.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.

	Command	Purpose
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**archive upload-sw rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***image-name***.tar**]	Upload the currently running access point image to the RCP server. • For **//***username*, specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-27. • For @*location*, specify the IP address of the RCP server. • For **/***directory*]**/***image-name***.tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. • The *image-name***.tar** is the name of software image to be stored on the server.

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Reloading the Image Using the Web Browser Interface

You can also use the Web browser interface to reload the access point image file. The Web broswer interface supports loading the image file using HTTP or TFTP interfaces.

Note Your access point configuration is not changed when using the browser to reload the image file.

Browser HTTP Interface

The HTTP interface allows you to browse to the access point image file on your PC and download the image to the access point. Follow the instructions below to use the HTTP interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **Browse** button to locate the image file on your PC.

Step 7 Click the **Upgrade** button.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the access point image file. Follow the instructions below to use a TFTP server:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **TFTP Upgrade** tab.

Step 7 Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the access point image file in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click the **Upgrade** button.

For additional information click the Help icon on the Software Upgrade screen.

CHAPTER 21

Configuring System Message Logging

This chapter describes how to configure system message logging on your access point.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This chapter consists of these sections:

- Understanding System Message Logging, page 21-2
- Configuring System Message Logging, page 21-2
- Displaying the Logging Configuration, page 21-12

Understanding System Message Logging

By default, access points send the output from system messages and **debug** privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

Note The syslog format is compatible with 4.3 BSD UNIX.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages are displayed on the console after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the console and each of the destinations. You can timestamp log messages or set the syslog source address to enhance real-time debugging and management.

You can access logged system messages by using the access point command-line interface (CLI) or by saving them to a properly configured syslog server. The access point software saves syslog messages in an internal buffer. You can remotely monitor system messages by accessing the access point through Telnet or by viewing the logs on a syslog server.

Configuring System Message Logging

This section describes how to configure system message logging. It contains this configuration information:

- System Log Message Format, page 21-2
- Default System Message Logging Configuration, page 21-3
- Disabling and Enabling Message Logging, page 21-4
- Setting the Message Display Destination Device, page 21-5
- Enabling and Disabling Timestamps on Log Messages, page 21-6
- Enabling and Disabling Sequence Numbers in Log Messages, page 21-6
- Defining the Message Severity Level, page 21-7
- Limiting Syslog Messages Sent to the History Table and to SNMP, page 21-8
- Setting a Logging Rate Limit, page 21-9
- Configuring UNIX Syslog Servers, page 21-10

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or timestamp information, if configured. Messages are displayed in this format:

seq no:timestamp: %facility-severity-MNEMONIC:description

The part of the message preceding the percent sign depends on the setting of the **service sequence-numbers**, **service timestamps log datetime**, **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**], or **service timestamps log uptime** global configuration command.

Table 21-1 describes the elements of syslog messages.

Table 21-1 System Log Message Elements

Element	Description
seq no:	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured. For more information, see the "Enabling and Disabling Sequence Numbers in Log Messages" section on page 21-6.
timestamp formats: *mm/dd hh:mm:ss* or *hh:mm:ss* (short uptime) or *d h* (long uptime)	Date and time of the message or event. This information appears only if the **service timestamps log** [**datetime** | **log**] global configuration command is configured. For more information, see the "Enabling and Disabling Timestamps on Log Messages" section on page 21-6.
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth). A facility can be a hardware device, a protocol, or a module of the system software. It denotes the source or the cause of the system message.
severity	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 21-3 on page 21-8.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

This example shows a partial access point system message:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Default System Message Logging Configuration

Table 21-2 shows the default system message logging configuration.

Table 21-2 Default System Message Logging Configuration

Feature	Default Setting
System message logging to the console	Enabled
Console severity	Debugging (and numerically lower levels; see Table 21-3 on page 21-8)
Logging buffer size	4096 bytes
Logging history size	1 message

Table 21-2 Default System Message Logging Configuration (continued)

Feature	Default Setting
Timestamps	Disabled
Synchronous logging	Disabled
Logging server	Disabled
Syslog server IP address	None configured
Server facility	Local7 (see Table 21-4 on page 21-11)
Server severity	Informational (and numerically lower levels; see Table 21-3 on page 21-8)

Disabling and Enabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Beginning in privileged EXEC mode, follow these steps to disable message logging:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no logging on**	Disable message logging.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config** or **show logging**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Disabling the logging process can slow down the access point because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.

The **logging synchronous** global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return. For more information, see the "Enabling and Disabling Timestamps on Log Messages" section on page 21-6.

To re-enable message logging after it has been disabled, use the **logging on** global configuration command.

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging buffered** [*size*] [*level*]	Log messages to an internal buffer. The default buffer size is 4096. The range is 4096 to 2147483647 bytes. Levels include emergencies 0, alerts 1, critical 2, errors 3, warnings 4, notifications 5, informational 6, and debugging 7. **Note** Do not make the buffer size too large because the access point could run out of memory for other tasks. Use the **show memory** privileged EXEC command to view the free processor memory on the access point; however, this value is the maximum available, and you should *not* set the buffer size to this amount.
Step 3	**logging** *host*	Log messages to a UNIX syslog server host. For *host*, specify the name or IP address of the host to be used as the syslog server. To build a list of syslog servers that receive logging messages, enter this command more than once. For complete syslog server configuration steps, see the "Configuring UNIX Syslog Servers" section on page 21-10.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**terminal monitor**	Log messages to a non-console terminal during the current session. Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The **logging buffered** global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging** privileged EXEC command. The first message displayed is the oldest message in the buffer. To clear the contents of the buffer, use the **clear logging** privileged EXEC command.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to a file, use the **no logging file** [*severity-level-number* | *type*] global configuration command.

Enabling and Disabling Timestamps on Log Messages

By default, log messages are not timestamped.

Beginning in privileged EXEC mode, follow these steps to enable timestamping of log messages:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**service timestamps log uptime** or **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]	Enable log timestamps. The first command enables timestamps on log messages, showing the time since the system was rebooted. The second command enables timestamps on log messages. Depending on the options selected, the timestamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable timestamps for both debug and log messages, use the **no service timestamps** global configuration command.

This example shows part of a logging display with the **service timestamps log datetime** global configuration command enabled:

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

This example shows part of a logging display with the s**ervice timestamps log uptime** global configuration command enabled:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Enabling and Disabling Sequence Numbers in Log Messages

Because there is a chance that more than one log message can have the same timestamp, you can display messages with sequence numbers so that you can unambiguously refer to a single message. By default, sequence numbers in log messages are not displayed.

Beginning in privileged EXEC mode, follow these steps to enable sequence numbers in log messages:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**service sequence-numbers**	Enable sequence numbers.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable sequence numbers, use the **no service sequence-numbers** global configuration command.

This example shows part of a logging display with sequence numbers enabled:

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Defining the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message, which are described in Table 21-3.

Beginning in privileged EXEC mode, follow these steps to define the message severity level:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging console** *level*	Limit messages logged to the console. By default, the console receives debugging messages and numerically lower levels (see Table 21-3 on page 21-8).
Step 3	**logging monitor** *level*	Limit messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels (see Table 21-3 on page 21-8).
Step 4	**logging trap** *level*	Limit messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels (see Table 21-3 on page 21-8). For complete syslog server configuration steps, see the "Configuring UNIX Syslog Servers" section on page 21-10.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config** or **show logging**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note Specifying a *level* causes messages at that level and numerically lower levels to be displayed at the destination.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to a terminal other than the console, use the **no logging monitor** global configuration command. To disable logging to syslog servers, use the **no logging trap** global configuration command.

Table 21-3 describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 21-3 Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The software generates four other categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**. These types of messages mean that the functionality of the access point is affected.
- Output from the **debug** commands, displayed at the **debugging** level. Debug commands are typically used only by the Technical Assistance Center (TAC).
- Interface up or down transitions and system restart messages, displayed at the **notifications** level. This message is only for information; access point functionality is not affected.
- Reload requests and low-process stack messages, displayed at the **informational** level. This message is only for information; access point functionality is not affected.

Limiting Syslog Messages Sent to the History Table and to SNMP

If you have enabled syslog message traps to be sent to an SNMP network management station by using the **snmp-server enable trap** global configuration command, you can change the level of messages sent and stored in the access point history table. You can also change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level **warning** and numerically lower levels (see Table 21-3 on page 21-8) are stored in the history table even if syslog traps are not enabled.

Beginning in privileged EXEC mode, follow these steps to change the level and history table size defaults:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging history** *level*[1]	Change the default level of syslog messages stored in the history file and sent to the SNMP server. See Table 21-3 on page 21-8 for a list of *level* keywords. By default, **warnings**, **errors**, **critical**, **alerts**, and **emergencies** messages are sent.
Step 3	**logging history size** *number*	Specify the number of syslog messages that can be stored in the history table. The default is to store one message. The range is 1 to 500 messages.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

1. Table 21-3 lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, emergencies equal 1, not 0, and critical equals 3, not 2.

When the history table is full (it contains the maximum number of message entries specified with the **logging history size** global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

To return the logging of syslog messages to the default level, use the **no logging history** global configuration command. To return the number of messages in the history table to the default value, use the **no logging history size** global configuration command.

Setting a Logging Rate Limit

You can enable a limit on the number of messages that the access point logs per second. You can enable the limit for all messages or for messages sent to the console, and you can specify that messages of a specific severity are exempt from the limit.

Beginning in privileged EXEC mode, follow these steps to enable a logging rate limit:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging rate-limit** *seconds* [**all**	**console**] [**except** *severity*]	Enable a logging rate limit in seconds. • (Optional) Apply the limit to all logging or only to messages logged to the console. • (Optional) Exempt a specific severity from the limit.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the rate limit, use the **no logging rate-limit** global configuration command.

Configuring UNIX Syslog Servers

The next sections describe how to configure the 4.3 BSD UNIX server syslog daemon and define the UNIX system logging facility.

Logging Messages to a UNIX Syslog Daemon

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server. Log in as root, and perform these steps:

Note Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX **man syslogd** command to determine what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

Step 1 Add a line such as the following to the file /etc/syslog.conf:

```
local7.debug /usr/adm/logs/cisco.log
```

The **local7** keyword specifies the logging facility to be used; see Table 21-4 on page 21-11 for information on the facilities. The **debug** keyword specifies the syslog level; see Table 21-3 on page 21-8 for information on the severity levels. The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

Step 2 Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /usr/adm/log/cisco.log
$ chmod 666 /usr/adm/log/cisco.log
```

Step 3 Make sure the syslog daemon reads the new changes by entering this command:

```
$ kill -HUP `cat /etc/syslog.pid`
```

For more information, see the **man syslog.conf** and **man syslogd** commands on your UNIX system.

Configuring the UNIX System Logging Facility

When sending system log messages to an external device, you can cause the access point to identify its messages as originating from any of the UNIX syslog facilities.

Beginning in privileged EXEC mode, follow these steps to configure UNIX system facility message logging:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging** *host*	Log messages to a UNIX syslog server host by entering its IP address. To build a list of syslog servers that receive logging messages, enter this command more than once.

	Command	Purpose
Step 3	**logging trap** *level*	Limit messages logged to the syslog servers. Be default, syslog servers receive informational messages and lower. See Table 21-3 on page 21-8 for *level* keywords.
Step 4	**logging facility** *facility-type*	Configure the syslog facility. See Table 21-4 on page 21-11 for *facility-type* keywords. The default is **local7**.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove a syslog server, use the **no logging** *host* global configuration command, and specify the syslog server IP address. To disable logging to syslog servers, enter the **no logging trap** global configuration command.

Table 21-4 lists the 4.3 BSD UNIX system facilities supported by the Cisco IOS software. For more information about these facilities, consult the operator's manual for your UNIX operating system.

Table 21-4 Logging Facility-Type Keywords

Facility Type Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Displaying the Logging Configuration

To display the current logging configuration and the contents of the log buffer, use the **show logging** privileged EXEC command. For information about the fields in this display, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

To display the logging history file, use the **show logging history** privileged EXEC command.

CHAPTER 22

Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following URL (select **Top Issues** and then select **Wireless Technologies)**:

http://www.cisco.com/tac

Sections in this chapter include:

- Checking the Top Panel Indicators, page 22-2
- Checking Basic Settings, page 22-5
- Resetting to the Default Configuration, page 22-5
- Reloading the Access Point Image, page 22-8

Checking the Top Panel Indicators

If your access point is not communicating, check the three LED indicators on the top panel to quickly assess the unit's status. Figure 22-1 shows the indicators on the 1200 series access point. Figure 22-2 shows the indicators on the 1100 series access point. Figure 22-3 and Figure 22-4 show the indicators on the 350 series access point.

Figure 22-1 Indicators on the 1200 Series Access Point

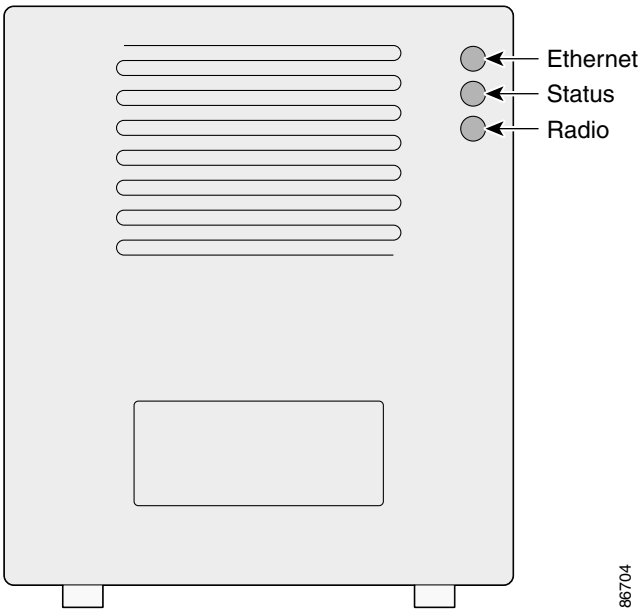


Figure 22-2 Indicators on the 1100 Series Access Point

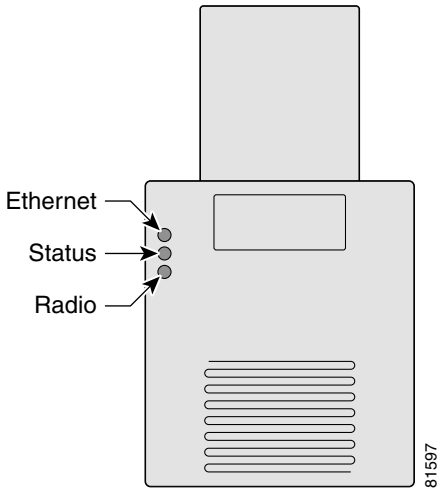


Figure 22-3 Indicators on the 350 Series Access Point (Plastic Case)

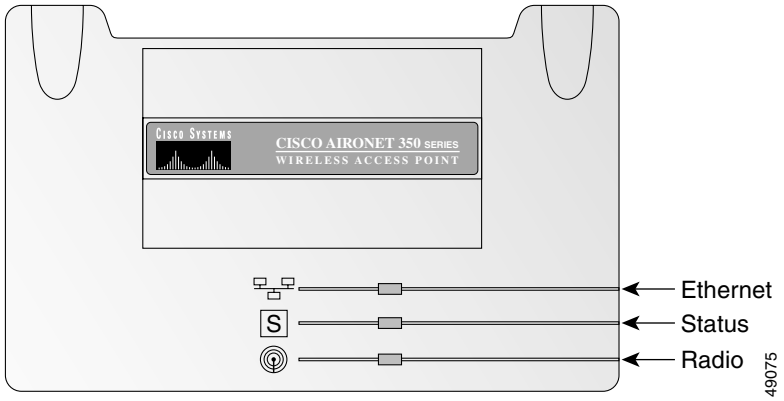
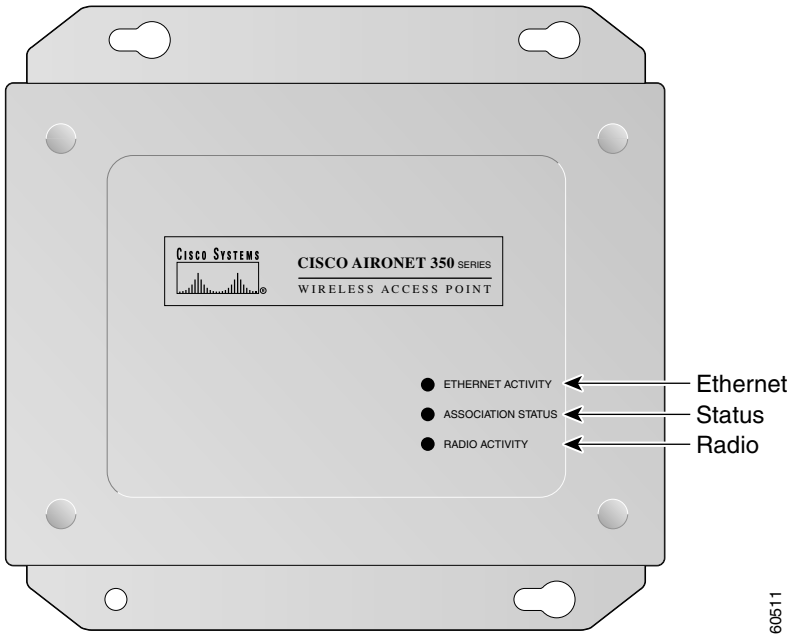


Figure 22-4 Indicators on the 350 Series Access Point (Metal Case)



The indicator signals have the following meanings (for additional details refer to Table 22-1):

- The Ethernet indicator signals traffic on the wired LAN. This indicator is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The indicator is off when the Ethernet cable is not connected.
- The status indicator signals operational status. Steady green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices.
- The radio indicator blinks green to indicate radio traffic activity. The light is normally off, but it blinks whenever a packet is received or transmitted over the access point's radio.

Table 22-1 Top Panel Indicator Signals

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test.
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS software.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	–	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failures	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
	Blinking red	–	–	Hardware failure. The access point must be replaced.
Firmware Upgrade	–	Red	–	Loading new firmware image.

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the access point does not communicate with client devices, check the following areas.

SSID

Wireless clients attempting to associate with the access point must use the same SSID as the access point. If a client device's SSID does not match the SSID of an access point in radio range, the client device will not associate. The access point default SSID is *tsunami*.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on your access point and any wireless devices with which it associates. For example, if you set WEP Key 3 on your client adapter to 0987654321 and select it as the transmit key, you must set WEP Key 3 on the access point to exactly the same value. The access point does not need to use Key 3 as its transmit key, however.

Refer to Chapter 9, "Configuring Cipher Suites and WEP," for instructions on setting the access point's WEP keys.

Security Settings

Wireless clients attempting to authenticate with your access point must support the same security options configured in the access point, such as EAP or LEAP, MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If a wireless client is unable to authenticate with your access point, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the access point settings.

Note The access point MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Resetting to the Default Configuration

If you forget the password that allows you to configure the access point, you may need to completely reset the configuration. On 1100 and 1200 series access points, you can use the MODE button on the access point or the web-browser interface. On 350 series access points, you can use the web-browser or CLI interfaces.

Note The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. The default username and password are both **Cisco**, which is case-sensitive.

Using the MODE Button

Follow these steps to delete the current configuration and return all access point settings to the factory defaults using the MODE button.

Note You cannot use the mode button to reset the configuration to defaults on 350 series access points. To reset the configuration on 350 series access points, follow the instructions in the "Using the Web Browser Interface" section on page 22-6, or in the "Using the CLI" section on page 22-7.

Step 1 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 2 Press and hold the **MODE** button while you reconnect power to the access point.

Step 3 Hold the **MODE** button until the Status LED turns amber (approximately 1 to 2 seconds), and release the button.

Step 4 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI.

Note The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP). The default username and password are **Cisco**, which is case-sensitive.

Using the Web Browser Interface

Follow these steps to delete the current configuration and return all access point settings to the factory defaults using the web browser interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click **System Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

Step 7 Click the **Reset to Defaults** button.

Note If the access point is configured with a static IP address, the IP address does not change.

Step 8 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI. The default username and password are **Cisco**, which is case-sensitive.

Using the CLI

Follow the steps below to delete the current configuration and return all access point settings to the factory defaults using the CLI.

Step 1 Open the CLI using a Telnet session or a connection to the access point console port.

Step 2 Reboot the access point by removing power and reapplying power.

Step 3 Let the access point boot until the command prompt appears and the access point begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...################################################################################
################################################################################
################################################################################
####################
```

Step 4 At the ap: prompt, enter the **flash_init** command to initialize the Flash.

```
ap: flash_init
Initializing Flash...
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
...done initializing Flash.
```

Step 5 Use the **dir flash:** command to display the contents of Flash and find the config.txt configuration file.

```
ap: dir flash:
Directory of flash:/
3 .rwx 223 <date> env_vars
4 .rwx 2190 <date> config.txt
5 .rwx 27 <date> private.config
150 drwx 320 <date> c350.k9w7.mx.122.13.JA
4207616 bytes available (3404800 bytes used)
```

Step 6 Use the **rename** command to change the name of the config.txt file to config.old.

```
ap: rename flash:config.txt flash:config.old
```

Step 7 Use the **reset** command to reboot the access point.

```
ap: reset
Are you sure you want to reset the system (y/n)?y
System resetting..Xmodem file system is available.
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
Reading cookie from flash parameter block...done.
```

```
Base ethernet MAC Address: 00:40:96:41:e4:df
Loading "flash:/c350.k9w7.mx.122.13.JA/c350.k9w7.mx.122.13.JA"...######## . . .
```

Note The access point is configured with factory default values, including the IP address (set to receive an IP address using DHCP) and the default username and password (**Cisco**).

Step 8 When IOS software is loaded, you can use the **del** privileged EXEC command to delete the config.old file from Flash.

```
ap# del flash:config.old
Delete filename [config.old]
Delete flash:config.old [confirm]
ap#
```

Reloading the Access Point Image

If your access point has a firmware failure, you must reload the complete access point image file using the Web browser interface or on 1100 and 1200 series access points, by pressing and holding the MODE button for around 30 seconds. You can use the browser interface if the access point firmware is still fully operational and you want to upgrade the firmware image. However, you can use the MODE button when the access point has a corrupt firmware image. On 350 series access points, you cannot use the MODE button to reload the image file, but you can use the CLI through a Telnet or console port connection.

Using the MODE button

You can use the MODE button on 1100 and 1200 series access points to reload the access point image file from an active Trivial File Transfer Protocol (TFTP) server on your network or on a PC connected to the access point Ethernet port.

Note You cannot use the mode button to reload the image file on 350 series access points. To reload the image file on 350 series access points, follow the instructions in the "Using the CLI" section on page 22-10.

Note If your access point experiences a firmware failure or a corrupt firmware image, indicated by three red LED indicators, you must reload the image from a connected TFTP server.

Note This process resets *all* configuration settings to factory defaults, including passwords, WEP keys, the access point IP address, and SSIDs.

Follow these steps to reload the access point image file:

Step 1 The PC you intend to use must be configured with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as *c1100-k9w7-tar.122-15.JA.tar* for an 1100 series access point or *c1200-k9w7-tar.122-15.JA.tar* for a 1200 series access point) in the TFTP server folder and that the TFTP server is activated. For additional information, refer to the "Obtaining the Access Point Image File" and "Obtaining TFTP Server Software" sections.

Step 3 Rename the access point image file in the TFTP server folder to **c1100-k9w7-tar.default** for an 1100 series access point or **c1200-k9w7-tar.default** for a 1200 series access point.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Step 7 Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI.

Using the Web Browser Interface

You can also use the Web browser interface to reload the access point image file. The Web broswer interface supports loading the image file using HTTP or TFTP interfaces.

Note Your access point configuration does not change when you use the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the access point image file on your PC and download the image to the access point. Follow the instructions below to use the HTTP interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click **Browse** to find the image file on your PC.

Step 7 Click **Upload**.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the access point image file. Follow the instructions below to use a TFTP server:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **TFTP Upgrade** tab.

Step 7 Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the access point image file in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click **Upload**.

For additional information click the **Help** icon on the Software Upgrade screen.

Using the CLI

Follow the steps below to reload the access point image using the CLI. When the access point begins to boot, you interrupt the boot process and use boot loader commands to load an image from a TFTP server to replace the image in the access point.

Note Your access point configuration is not changed when using the CLI to reload the image file.

Step 1 Open the CLI using a Telnet session or a connection to the access point console port.

Step 2 Reboot the access point by removing power and reapplying power.

Step 3 Let the access point boot until it begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...################################################################################
################################################################################
################################################################################
####################
```

Step 4 When the ap: command prompt appears, enter the **set** command to assign an IP address, subnet mask, and default gateway to the access point.

Note You must use upper-case characters when you enter the **IP-ADDR**, **NETMASK**, and **DEFAULT_ROUTER** options with the **set** command.

Your entries might look like this example:

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

Step 5 Enter the **tftp_init** command to prepare the access point for TFTP.

```
ap: tftp_init
```

Step 6 Enter the **tar** command to load and inflate the new image from your TFTP server. The command must include this information:

- the **-xtract** option, which inflates the image when it is loaded
- the IP address of your TFTP server
- the directory on the TFTP server that contains the image
- the name of the image
- the destination for the image (the access point Flash)

Your entry might look like this example:

```
ap: tar -xtract tftp://192.168.130.222/images/c350-k9w7-tar.122-13.JA1 flash:
```

Step 7 When the display becomes full the CLI pauses and displays `--MORE--`. Press the spacebar to continue.

```
extracting info (229 bytes)
c350-k9w7-mx.122-13.JA1/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/level1/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/appsui.js (558 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/back.htm (205 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/cookies.js (5027 bytes).
extracting c350-k9w7-mx.122-13.JA1/html/level1/forms.js (15704 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/sitewide.js (14621 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/config.js (2554 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/stylesheet.css (3215 bytes)
c350-k9w7-mx.122-13.JA1/html/level1/images/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/ap_title_appname.gif (1422 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_1st.gif (1171 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_cbottom.gif (318 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_current.gif (348 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last.gif (386 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_filler.gif (327
bytes)
```

```
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_flat.gif (318
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_nth.gif (1177 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_leftnav_dkgreen.gif (869 bytes)
 -- MORE --
```

If you do not press the spacebar to continue, the process eventually times out and the access point stops inflating the image.

Step 8 Enter the **set BOOT** command to designate the new image as the image that the access point uses when it reboots. The access point creates a directory for the image that has the same name as the image, and you must include the directory in the command. Your entry might look like this example:

```
ap: set BOOT flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
```

Step 9 Enter the **set** command to check your bootloader entries.

```
ap: set
BOOT=flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
DEFAULT_ROUTER=192.168.133.1
IP_ADDR=192.168.133.160
NETMASK=255.255.255.0
```

Step 10 Enter the **boot** command to reboot the access point. When the access point reboots, it loads the new image.

```
ap: boot
```

Obtaining the Access Point Image File

You can obtain the access point image file from the Cisco.com software center by following these steps:

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

http://www.cisco.com/public/sw-center/sw-wireless.shtml

Step 2 Find the access point firmware and utilities section and click on the link for the 350, 1100, or 1200 series access point.

Step 3 Double-click the latest firmware image file, such as *c1100-k9w7-tar.122-11.JA* for 1100 series access points or *c1200-k9w7-tar.122-11.JA* for 1200 series access points.

Step 4 Download the access point image file to a directory on your PC hard drive.

Obtaining TFTP Server Software

You can download TFTP server software from several websites. Cisco recommends the shareware TFTP utility available at this URL:

http://tftpd32.jounin.net

Follow the instructions on the website for installing and using the utility.

Channels and Antenna Settings

This appendix lists the access point radio channels and the maximum power levels supported by the world's regulatory domains.

The following topics are covered in this appendix:

- Channels, page A-2
- Maximum Power Levels and Antenna Gains, page A-5

Channels

IEEE 802.11b (2.4-GHz Band)

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11b 22-MHz-wide channel are shown in Table A-1.

Table A-1 Channels for IEEE 802.11b

Channel Identifier	Center Frequency (MHz)	Regulatory Domains				
		Americas (–A)	EMEA (–E)	Japan (–J)	Israel (–I)	China (–C)
1	2412	X	X	X	–	X
2	2417	X	X	X	–	X
3	2422	X	X	X	–	X
4	2427	X	X	X	–	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	–	X
10	2457	X	X	X	–	X
11	2462	X	X	X	–	X
12	2467	–	X	X	–	–
13	2472	–	X	X	–	–
14	2484	–	-	X	–	–

Note Mexico is included in the Americas (–A) regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of Mexico.

IEEE 802.11g (2.4-GHz Band)

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11g 22-MHz-wide channel are shown in Table A-2.

Table A-2 Channels for IEEE 802.11g

Channel Identifier	Center Frequency (MHz)	Regulatory Domains							
		Americas (–A)		EMEA (–E)		Israel (–I)		Japan (–J)	
		CCK	OFDM	CCK	OFDM	CCK	OFDM	CCK	OFDM
1	2412	X	X	X	X	–	–	X	X
2	2417	X	X	X	X	–	–	X	X
3	2422	X	X	X	X	–	–	X	X
4	2427	X	X	X	X	–	–	X	X
5	2432	X	X	X	X	X	X	X	X
6	2437	X	X	X	X	X	X	X	X
7	2442	X	X	X	X	X	X	X	X
8	2447	X	X	X	X	X	X	X	X
9	2452	X	X	X	X	–	–	X	X
10	2457	X	X	X	X	–	–	X	X
11	2462	X	X	X	X	–	–	X	X
12	2467	–	–	X	X	–	–	X	X
13	2472	–	–	X	X	–	–	X	X
14	2484	–	–	–	–	–	–	X	–

IEEE 802.11a (5-GHz Band)

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11a 20-MHz-wide channel are shown in Table A-3.

Table A-3 Channels for IEEE 802.11a

Channel Identifier	Center Frequency (MHz)	Regulatory Domains			
		Americas (–A)	Japan (–J)	Singapore (–S)	Taiwan (–T)
34	5170	–	X	–	–
36	5180	X	–	X	–
38	5190	–	X	–	–
40	5200	X	–	X	–
42	5210	–	X	–	–
44	5220	X	–	X	–
46	5230	–	X	–	–
48	5240	X	-	X	–
52	5260	X	–	–	X
56	5280	X	–	–	X
60	5300	X	–	–	X
64	5320	X	–	–	X

Note All channel sets are restricted to indoor usage except the Americas (–A), which allows for indoor and outdoor use on channels 52 through 64 in the United States.

Maximum Power Levels and Antenna Gains

IEEE 802.11b (2.4-GHz Band)

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table A-4 indicates the maximum power levels and antenna gains allowed for each IEEE 802.11b regulatory domain.

Table A-4 Maximum Power Levels Per Antenna Gain for IEEE 802.11b

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Americas (–A) (4W EIRP maximum)	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
EMEA (–E) (100 mW EIRP maximum)	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
Japan (–J) (10 mW/MHz EIRP maximum)	2.2	30
	5.2	30
	6	30
	8.5	n/a
	12	n/a
	13.5	5
Israel (–I) (100 mW EIRP maximum)	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5

IEEE 802.11g (2.4-GHz Band)

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table A-5 indicates the maximum power levels and antenna gains allowed for each IEEE 802.11g regulatory domain.

Table A-5 Maximum Power Levels Per Antenna Gain for IEEE 802.11g

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)	
		CCK	OFDM
Americas (–A) (4W EIRP maximum)	2.2	100	30
	5.2	100	30
	6	100	30
	8.5	100	30
	10	100	30
EMEA (–E) (100 mW EIRP maximum)	2.2	50	30
	5.2	30	10
	6	30	10
	8.5	10	5
	10	10	5
Japan (–J) (10 mW/MHz EIRP maximum)	2.2	30	30
	5.2	30	30
	6	30	30
	8.5	n/a	n/a
	10	n/a	n/a
Israel (–I) (100 mW EIRP maximum)	2.2	50	30
	5.2	30	10
	6	30	10
	8.5	10	5
	10	10	5

IEEE 802.11a (5-GHz Band)

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table A-6 indicates the maximum power levels allowed with the Cisco integrated antenna for each IEEE 802.11a regulatory domain.

Table A-6 Maximum Power Levels Per Antenna Gain for IEEE 802.11a

Regulatory Domain	Maximum Power Level (mW) with 6-dBi Antenna Gain
Americas (–A) (160 mW EIRP maximum on channels 36-48, (800 mW EIRP maximum on channels 52-64)	40
Japan (–J) (10 mW/MHz EIRP maximum)	40
Singapore (–S) (100 mW EIRP maximum)	20
Taiwan (–T) (800 mW EIRP maximum)	40

Protocol Filters

The tables in this appendix list some of the protocols that you can filter on the access point. The tables include:

- Table E-1, Ethertype Protocols
- Table E-2, IP Protocols
- Table E-3, IP Port Protocols

In each table, the Protocol column lists the protocol name, the Additional Identifier column lists other names for the same protocol, and the ISO Designator column lists the numeric designator for each protocol.

Table B-1 Ethertype Protocols

Protocol	Additional Identifier	ISO Designator
ARP	—	0x0806
RARP	—	0x8035
IP	—	0x0800
Berkeley Trailer Negotiation	—	0x1000
LAN Test	—	0x0708
X.25 Level3	X.25	0x0805
Banyan	—	0x0BAD
CDP	—	0x2000
DEC XNS	XNS	0x6000
DEC MOP Dump/Load	—	0x6001
DEC MOP	MOP	0x6002
DEC LAT	LAT	0x6004
Ethertalk	—	0x809B
Appletalk ARP	Appletalk AARP	0x80F3
IPX 802.2	—	0x00E0
IPX 802.3	—	0x00FF
Novell IPX (old)	—	0x8137
Novell IPX (new)	IPX	0x8138
EAPOL (old)	—	0x8180
EAPOL (new)	—	0x888E
Telxon TXP	TXP	0x8729
Aironet DDP	DDP	0x872D
Enet Config Test	—	0x9000
NetBUI	—	0xF0F0

Table B-2 IP Protocols

Protocol	Additional Identifier	ISO Designator
dummy	—	0
Internet Control Message Protocol	ICMP	1
Internet Group Management Protocol	IGMP	2
Transmission Control Protocol	TCP	6
Exterior Gateway Protocol	EGP	8
PUP	—	12
CHAOS	—	16
User Datagram Protocol	UDP	17
XNS-IDP	IDP	22
ISO-TP4	TP4	29
ISO-CNLP	CNLP	80
Banyan VINES	VINES	83
Encapsulation Header	encap_hdr	98
Spectralink Voice Protocol	SVP Spectralink	119
raw	—	255

Table B-3 IP Port Protocols

Protocol	Additional Identifier	ISO Designator
TCP port service multiplexer	tcpmux	1
echo	—	7
discard (9)	—	9
systat (11)	—	11
daytime (13)	—	13
netstat (15)	—	15
Quote of the Day	qotd quote	17
Message Send Protocol	msp	18
ttytst source	chargen	19
FTP Data	ftp-data	20
FTP Control (21)	ftp	21
Secure Shell (22)	ssh	22
Telnet	—	23
Simple Mail Transport Protocol	SMTP mail	25
time	timserver	37
Resource Location Protocol	RLP	39
IEN 116 Name Server	name	42
whois	nicname 43	43
Domain Name Server	DNS domain	53
MTP	—	57
BOOTP Server	—	67
BOOTP Client	—	68
TFTP	—	69
gopher	—	70
rje	netrjs	77
finger	—	79
Hypertext Transport Protocol	HTTP www	80
ttylink	link	87
Kerberos v5	Kerberos krb5	88
supdup	—	95
hostname	hostnames	101

Table B-3 IP Port Protocols (continued)

Protocol	Additional Identifier	ISO Designator
TSAP	iso-tsap	102
CSO Name Server	cso-ns csnet-ns	105
Remote Telnet	rtelnet	107
Postoffice v2	POP2 POP v2	109
Postoffice v3	POP3 POP v3	110
Sun RPC	sunrpc	111
tap ident authentication	auth	113
sftp	—	115
uucp-path	—	117
Network News Transfer Protocol	Network News readnews nntp	119
USENET News Transfer Protocol	Network News readnews nntp	119
Network Time Protocol	ntp	123
NETBIOS Name Service	netbios-ns	137
NETBIOS Datagram Service	netbios-dgm	138
NETBIOS Session Service	netbios-ssn	139
Interim Mail Access Protocol v2	Interim Mail Access Protocol IMAP2	143
Simple Network Management Protocol	SNMP	161
SNMP Traps	snmp-trap	162
ISO CMIP Management Over IP	CMIP Management Over IP cmip-man CMOT	163
ISO CMIP Agent Over IP	cmip-agent	164
X Display Manager Control Protocol	xdmcp	177
NeXTStep Window Server	NeXTStep	178
Border Gateway Protocol	BGP	179
Prospero	—	191
Internet Relay Chap	IRC	194

Table B-3 IP Port Protocols (continued)

Protocol	Additional Identifier	ISO Designator
SNMP Unix Multiplexer	smux	199
AppleTalk Routing	at-rtmp	201
AppleTalk name binding	at-nbp	202
AppleTalk echo	at-echo	204
AppleTalk Zone Information	at-zis	206
NISO Z39.50 database	z3950	210
IPX	—	213
Interactive Mail Access Protocol v3	imap3	220
Unix Listserv	ulistserv	372
syslog	—	514
Unix spooler	spooler	515
talk	—	517
ntalk	—	518
route	RIP	520
timeserver	timed	525
newdate	tempo	526
courier	RPC	530
conference	chat	531
netnews	—	532
netwall	wall	533
UUCP Daemon	UUCP uucpd	540
Kerberos rlogin	klogin	543
Kerberos rsh	kshell	544
rfs_server	remotefs	556
Kerberos kadmin	kerberos-adm	749
network dictionary	webster	765
SUP server	supfilesrv	871
swat for SAMBA	swat	901
SUP debugging	supfiledbg	1127
ingreslock	—	1524
Prospero non-priveleged	prospero-np	1525
RADIUS	—	1812
Concurrent Versions System	CVS	2401
Cisco IAPP	—	2887
Radio Free Ethernet	RFE	5002

Supported MIBs

This appendix lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the access point supports for this software release. The Cisco IOS SNMP agent supports both SNMPv1 and SNMPv2. This appendix contains these sections:

- MIB List, page C-1
- Using FTP to Access the MIB Files, page C-2

MIB List

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-L2-DEV-MONITORING-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOL-FILTER-MIB
- CISCO-SYSLOG-EVENT-EXT-MIB
- CISCO-TBRIDGE-DEV-IF-MIB
- BRIDGE-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB

- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-SMI-MIB
- CISCO-TC-MIB
- CISCO-SYSLOG-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RFC1398-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC

Using FTP to Access the MIB Files

Follow these steps to obtain each MIB file by using FTP:

Step 1 Use FTP to access the server **ftp.cisco.com**.

Step 2 Log in with the username **anonymous**.

Step 3 Enter your e-mail username when prompted for the password.

Step 4 At the `ftp>` prompt, change directories to **/pub/mibs/v1** or **/pub/mibs/v2**.

Step 5 Use the **get** *MIB_filename* command to obtain a copy of the MIB file.

Note You can also access information about MIBs on the Cisco web site:
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Error and Event Messages

This appendix lists the CLI error and event messages.

Software Auto Upgrade Messages

Error Message `SW_AUTO_UPGRADE-FATAL: Attempt to upgrade software failed, software on Flash may be deleted. Please copy software into Flash.`

Explanation Auto upgrade of the software failed. The software on the Flash memory might have been deleted. Copy software into the Flash memory.

Recommended Action Copy software before rebooting the unit.

Error Message `SW_AUTO_UPGRADE-7-FAILURE: dhcp_client_start_stop failed`

Explanation Auto upgrade of the software failed due to error in starting/stopping DHCP client process.

Recommended Action Copy the error message exactly as it appears and report it to your technical support representative.

Error Message `SW_AUTO_UPGRADE-7-FAILURE: Failed to obtain ip addr from dhcp server`

Explanation Auto upgrade of the software failed.

Recommended Action Copy the error message exactly as it appears and report it to your technical support representative.

Error Message `SW_AUTO_UPGRADE-7-FAILURE: boot_file_pathent creation failed`

Explanation Auto upgrade of the software failed due to error in creation of pathent (internal data structure).

Recommended Action Copy the error message exactly as it appears and report it to your technical support representative.

Association Management Messages

Error Message `DOT11-3-BADSTATE: [mac-address] [chars] [chars] -> [chars]`

Explanation 802.11 Association and management uses a table-driven state machine to keep track and transition an Association through various states. A state transition occurs when an Association receives one of many possible events. When this error occurs, it means that an Association received an event that it did not expect while in this state.

Recommended Action The system can continue but may lose the Association that generates this error. Copy the message exactly as it appears and report it to your technical service representative.

Error Message `DOT11-6-ASSOC: Interface [interface], Station [char] [mac] Associated`

Explanation A station associated to an access point.

Recommended Action None.

Error Message `DOT11-6-ADD: Interface [interface], Station [mac] Associated to Parent [mac]`

Explanation A station associated to an access point.

Recommended Action None.

Error Message `DOT11-6-DISASSOC: Interface [interface], Deauthenticating Station [mac] [char]`

Explanation A station disassociated from an access point.

Recommended Action None.

Error Message `DOT11-6-ROAMED: Station [mac-address] Roamed to [mac-address]`

Explanation A station roamed to a new access point.

Recommended Action None.

Proxy Mobile IP Subsystem Messages

Error Message `PMIP-3-REG_FAIL: Mobile Node 10.4.1.3 mobile ip registration failed`

Explanation When a mobile node (MN) moves to a foreign network, the access point registers the MN to its Home Agent. This message indicates that the registration failed.

Recommended Action Verify correct configuration of Mobile IP agents and the access point.

Error Message `PMIP-3-REG_AUTH_FAIL: Mobile Node 10.4.1.3 registration failed due to authentication failure`

Explanation When a mobile node (MN) moves to a foreign network, the access point registers the MN to its Home Agent. This message indicates that the registration failed because the HA or FA failed to authenticate each other or the MN.

Recommended Action Verify that the correct authentication information is configured on the Home Agent, the Foreign Agent, and the access point.

Error Message `PMIP-3-REG_FA_FAIL: Mobile Node 10.4.1.3 registration failed due to Foreign Agent denial`

Explanation When a Mobile node (MN) moves to a foreign network, the access point registers the MN to its Home Agent. This message indicates that the registration was denied by the Foreign Agent.

Recommended Action Make sure the correct authentication information is configured on the Home Agent, the Foreign Agent, and the access point.

Error Message `PMIP-3-REG_HA_FAIL: Mobile Node 10.4.1.3 registration failed due to Home Agent denial`

Explanation When a Mobile node (MN) moves to a foreign network, the access point registers the MN to its Home Agent. This message indicates that the registration was denied by the Home Agent.

Recommended Action Make sure the correct authentication information is configured on the Home Agent, the Foreign Agent, and the access point.

Error Message `PMIP-3-AUTH_UNAVAIL: Authentication for 10.4.1.3 unavailable`

Explanation Proxy Mobile IP failed to obtain the Mobile Node's authentication information either locally or from a AAA server.

Recommended Action Make sure the correct Mobile Node information is configured locally or on the AAA server.

Error Message `PMIP-3-HAFA_UNAVAIL: No response from the Mobile IP Agent to our registration requests`

Explanation Proxy Mobile IP failed to access the Home or Foreign Agent while trying to register the Mobile Node.

Recommended Action Make sure the HA or FA is not down or is network inaccessible. Also check that the subnet map information regarding the Home Agent is correct.

Error Message `PMIP-6-HAFA_DOWN: Mobile IP Agent 10.4.1.1 is down or unavailable`

Explanation Mobile IP Home or Foreign agent has gone down or is inaccessible to the access point.

Recommended Action Make sure there is at least one Home and Foreign Agent configured on that subnet and is accessible to the access point.

Error Message `PMIP-3-AAP_UNAVAIL: Authoritative Access Point is unavailable`

Explanation The authoritative access point cannot be reached to obtain the subnet map table.

Recommended Action Make sure all the access points have the same information regarding authoritative and regular access points.

Error Message `PMIP-6-START: Proxy Mobile IP services has started`

Explanation Proxy Mobile IP service has started.

Recommended Action None.

Error Message `PMIP-6-STOP: Proxy Mobile IP services have stopped`

Explanation Proxy Mobile IP service has stopped.

Recommended Action None.

Error Message `PMIP-6-REPEATER_STOP: AP is now operating as a repeater, disabling Proxy Mobile IP services`

Explanation Proxy Mobile IP does not run on repeaters or workgroup bridges, and it is disabled automatically when the access point is in repeater mode.

Recommended Action None.

Error Message `PMIP-3-SM_SOCKET_ERR: Subnet Map Socket Open failed, IP address may not be set`

Explanation The subnet map features does not work properly when a subnet map socket is not created.

Recommended Action Make sure that the access point has an IP address.

Unzip Messages

Error Message `SOAP-4-UNZIP_OVERFLOW: Failed to unzip Flash:/c1200-k9w7-mx.122-3.6.JA1/html/level15/ap_xxx.htm.gz, exceeds maximum uncompressed html size`

Explanation The HTTP server cannot retrieve a compressed file in response to an HTTP GET request because the size of the file is too large for the buffers used in the uncompression process.

Recommended Action Make sure file is a valid HTML page. If so, you'll have to copy an uncompressed version of the file into Flash to retrieve it through HTTP.

802.11 Subsystem Messages

Error Message `DOT11-6-FREQ_INUSE: Radio frequency [int] is in use`

Explanation When scanning for an unused frequency, the unit recognized another radio using the displayed frequency.

Recommended Action None.

Error Message `DOT11-6-FREQ_USED: Radio frequency [int] selected`

Explanation After scanning for an unused frequency, the unit selected the displayed frequency.

Recommended Action None.

Error Message `DOT11-4-NO_VALID_INFRA_SSID: Interface [interface] no valid infrastructure SSID configured, radio not started`

Explanation For the access point to function as a repeater, at least one active SSID must be designated as an infrastructure SSID.

Recommended Action Add at least one infrastructure SSID to the radio configuration.

Error Message `DOT11-4-VERSION_MISMATCH: Require radio version [hex].[int], found version [hex].[int]`

Explanation When starting the radio, the access point found the wrong firmware version. The radio will be loaded with the required version.

Recommended Action None.

Error Message `DOT11-4-VERSION_UPGRADE: Interface [number], upgrading radio firmware`

Explanation When starting the radio, the access point found the wrong firmware version. The radio will be loaded with the required version.

Recommended Action None.

Error Message `DOT11-2-VERSION_INVALID: Unable to find required radio version [hex].[int]`

Explanation When trying to re-flash the radio firmware, the access point recognized that the radio firmware packaged with the Cisco IOS software had the incorrect version.

Recommended Action None.

Error Message `DOT11-4-NO_SSID: No SSIDs configured, radio not started`

Explanation All SSIDs were deleted from the configuration. At least one must be configured for the radio to run.

Recommended Action Configure at least one SSID on the access point.

Error Message `DOT11-4-FLASHING_RADIO: Flashing the radio firmware ([chars])`

Explanation The radio has been stopped to load new firmware.

Recommended Action None.

Error Message `DOT11-4-LOADING_RADIO: Interface [interface] loading the radio firmware ([chars])`

Explanation The radio has been stopped to load new firmware.

Recommended Action None.

Error Message `DOT11-2-NO_FIRMWARE: No radio firmware file ([chars]) was found`

Explanation When trying to Flash new firmware into the radio, the file for the radio was not found in the Flash file system.

Recommended Action The wrong image has been loaded into the unit. Locate the correct image based on the type of radio used.

Error Message `DOT11-2-BAD_FIRMWARE: Radio firmware file ([chars]) is invalid`

Explanation When trying to Flash new firmware into the radio, the file was found to be invalid.

Recommended Action Put the correct firmware image file in the place where the unit is looking.

Error Message `DOT11-2-RADIO_FAILED: Interface [interface] failed — [chars]`

Explanation The radio driver found a severe error and is shutting down.

Recommended Action None.

Error Message `DOT11-4-FLASH_RADIO_DONE: Flashing the radio firmware completed`

Explanation The radio firmware Flash is complete, and the radio will be restarted with the new firmware.

Recommended Action None.

Error Message `DOT11-4-LINK_DOWN: Radio parent lost: [chars]`

Explanation The connection to the parent access point was lost for the displayed reason. The unit will try to find a new parent access point.

Recommended Action None.

Error Message `DOT11-4-CANT_ASSOC: Cannot associate: [chars]`

Explanation The unit could not establish a connection to a parent access point for the displayed reason.

Recommended Action Verify that the basic configuration settings (SSID, WEP, and others) of the parent access point and this unit match.

Error Message `DOT11-4-MAXRETRIES: Packet to client [mac] reached max retries, remove the client`

Explanation A packet sent to the client has not been successfully delivered many times, and the max retries limit has been reached. The client is deleted from the association table.

Recommended Action None.

Error Message `DOT11-4-BRIDGE_LOOP: Bridge loop detected between WGB [mac-address] and device [mac-address]`

Explanation A workgroup bridge reported the address of one of its Ethernet clients and the access point already had that address marked as being somewhere else on the network.

Recommended Action Click **Refresh** on the Associations page on the access point GUI, or enter the **clear dot11 statistics** command on the CLI.

Error Message `DOT11-3-RF_LOOPBACK_FAILURE: Interface [number] Radio failed to pass RF loopback test`

Explanation Radio loopback test failed for a radio interface.

Recommended Action None.

Error Message `DOT11-3-RF_LOOPBACK__FREQ_FAILURE: Radio failed to pass RF loopback test at freq [frequency]`

Explanation Radio loopback test failed at a given frequency.

Recommended Action None.

Error Message `DOT11-AUTH_FAILED: Station [mac-address] authentication failed`

Explanation The station failed authentication.

Recommended Action Verify that the user entered the correct username and password, and check that the authentication server is online.

Error Message `DOT11-CCKM_AUTH_FAILED: Station [mac-address] CCKM authentication failed`

Explanation The station failed CCKM authentication.

Recommended Action Verify that the topology of the access points configured to use the WDS access point is functional.

Error Message `DOT11-TKIP_MIC_FAILURE: TKIP Michael MIC failure was detected on a packet (TSC=0x0) received from [mac-address]`

Explanation TKIP Michael MIC failure was detected on a unicast frame decrypted locally with the pairwise key.

Recommended Action A failure of the Michael MIC in a packet usually indicates an active attack on your network. Search for and remove potential rogue devices from your wireless LAN.

Error Message `DOT11-TKIP_MIC_FAILURE_REPORT: Received TKIP Michael MIC failure report from the station [mac-address] on the packet (TSC=0x0) encrypted and protected by [key] key`

Explanation The access point received an EAPOL-key from a station notifying the access point that TKIP Michael MIC failed on a packet transmitted by this access point.

Recommended Action None.

Error Message `DOT11-TKIP_MIC_FAILURE_REPEATED: Two TKIP Michael MIC failures were detected within [number] seconds on [interface] interface. The interface will be put on MIC failure hold state for next [number] seconds`

Explanation Because MIC failures usually indicate an active attack on your network, the interface will be put on hold for the configured time. During this hold time, stations using TKIP ciphers are disassociatedand cannot reassociate until the hold time ends. At the end of the hold time, the interface operates normally.

Recommended Action Michael MIC failures usually indicate an active attack on your network. Search for and remove potential rogue devices from your wireless LAN. If this is a false alarm and the interface should not be on hold this long, use the **countermeasure tkip hold-time** command to adjust the hold time.

Inter-Access Point Protocol Messages

Error Message `DOT11-6-ROAMED: Station [mac-address] Roamed to [mac-address]`

Explanation A station has roamed to a new access point.

Recommended Action None.

Error Message `DOT11-6-STANDBY_ACTIVE: Standby to Active, Reason = [chars] ([int])`

Explanation The access point is transitioning from standby mode to active mode.

Recommended Action None.

Error Message `DOT11-6-ROGUE_AP: Rogue AP [mac-address] reported. Reason: [chars]`

Explanation A station has reported a potential rogue access point for the stated reason.

Recommended Action None.

Error Message `SCHED-3-UNEXPECTEDMESSAGE: Unknown message [hex] received (ptr arg [hex], num arg [hex]).`

Explanation A process can register to be notified when various events occur in the router. This message indicates that a process received a message from another process that it does not know how to handle.

Recommended Action Copy the error message exactly as it appears, and report it to your technical support representative.

Error Message `SCHED-3-UNEXPECTEDEVENT: Process received unknown event (maj [hex], min [hex]).`

Explanation A process can register to be notified when various events occur in the router. This message indicates that a process received an event that it did not know how to handle.

Recommended Action Copy the error message exactly as it appears, and report it to your technical support representative.

Error Message `DOT11-STANDBY-REQUEST: Hotstandby request to shut down radios from [mac-address]`

Explanation A standby access point has requested this access point to shut down its radio interfaces because a failure has been detected on one of this access point's radio interfaces.

Recommended Action None.

Radio Diagnostic Messages

Error Message `DOT11-4-RM_INCAPABLE: Interface [interface]`

Explanation This interface has been requested to send a radio management request, but this interface does not support radio management.

Recommended Action None.

Error Message `DOT11-RM-INCORRECT-INTERFACE: Invalid interface, either not existing or non-radio`

Explanation This interface has been requested to send a radio management request, but this interface either does not exist or is not a radio interface.

Recommended Action None.

Local Authenticator Messages

Error Message `RADSRV-4-NAS_UNKNOWN: Unknown authenticator: [ip-address]`

Explanation The local RADIUS server received an authentication request but does not recognize the IP address of the network access server (NAS) that forwarded the request.

Recommended Action Make sure that every access point on your wireless LAN is configured as a NAS on your local RADIUS server.

802.11 The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.

802.11a The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency band.

802.11b The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs operating in the 2.4-GHz frequency band.

A

access point A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.

ad hoc network A wireless network composed of stations without Access Points.

antenna gain The gain of an antenna is a measure of the antenna's ability to direct or focus radio energy over a region of space. High gain antennas have a more focused radiation pattern in a specific direction.

associated A station is configured properly to allow it to wirelessly communicate with an Access Point.

B

backoff time The random length of time that a station waits before sending a packet on the LAN. Backoff time is a multiple of slot time, so a decrease in slot time ultimately decreases the backoff time, which increases throughput.

beacon A wireless LAN packet that signals the availability and presence of the wireless device. Beacon packets are sent by access points and base stations; however, client radio cards send beacons when operating in computer to computer (Ad Hoc) mode.

BOOTP Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.

BPSK A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.

broadcast packet A single data message (packet) sent to all addresses on the same subnet.

C

CCK Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.

CCKM Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.

cell The area of radio range or coverage in which the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.

client A radio device that uses the services of an Access Point to communicate wirelessly with other devices on a local area network.

CSMA Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

D

data rates The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dBi A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.

DHCP Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

dipole A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.

domain name The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider (such as an ISP); name.ar—Argentina; name.au—Australia; and so on.

DNS Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.

DSSS Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

E

EAP Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.

Ethernet The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 Mbps, depending on the physical layer used.

F

file server A repository for files so that a local area network can share files, mail, and programs.

firmware Software that is programmed on a memory chip.

G

gateway A device that connects two otherwise incompatible networks together.

GHz Gigahertz. One billion cycles per second. A unit of measure for frequency.

I

IEEE Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

infrastructure The wired Ethernet network.

IP address The Internet Protocol (IP) address of a station.

IP subnet mask The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address; for example: 255.255.255.0.

isotropic An antenna that radiates its signal in a spherical pattern.

M

MAC Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or your client adapter.

modulation Any of several techniques for combining user information with a transmitter's carrier signal.

multipath The echoes created as a radio signal bounces off of physical objects.

multicast packet A single data message (packet) sent to multiple addresses.

O

omni-directional This typically refers to a primarily circular antenna radiation pattern.

Orthogonal Frequency Division Multiplex (OFDM) A modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

P

packet A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Q

Quadruple Phase Shift Keying A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.

R

range A linear measure of the distance that a transmitter can send a signal.

receiver sensitivity A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

RF Radio frequency. A generic term for radio-based technology.

roaming A feature of some Access Points that allows users to move through a facility while maintaining an unbroken connection to the LAN.

RP-TNC A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.

S

slot time The amount of time a device waits after a collision before retransmitting a packet. Short slot times decrease the backoff time, which increases throughput.

spread spectrum A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

SSID Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

T

transmit power The power level of radio transmission.

U

UNII Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15 to 5.35 GHz and 5.725 to 5.825 GHz frequency bands.

UNII-1 Regulations for UNII devices operating in the 5.15 to 5.25 GHz frequency band.

UNII-2 Regulations for UNII devices operating in the 5.25 to 5.35 GHz frequency band.

UNII-3 Regulations for UNII devices operating in the 5.725 to 5.825 GHz frequency band.

unicast packet A single data message (packet) sent to a specific IP address.

W

WDS Wireless Domain Services (WDS). An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.

WEP Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.

WLSE Wireless LAN Solutions Engine. The WLSE is a specialized appliance for managing Cisco Aironet wireless LAN infrastructures. It centrally identifies and configures access points in customer-defined groups and reports on throughput and client associations. WLSE's centralized management capabilities are further enhanced with an integrated template-based configuration tool for added configuration ease and improved productivity.

WNM Wireless Network Manager.

workstation A computing device with an installed client adapter.

WPA Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

A

abbreviating commands 4-3
access point image 22-8
access point security settings, matching client devices 10-17
accounting
  with RADIUS 12-12
  with TACACS+ 12-21, 12-26
AES-CCMP 9-2
antenna
  gains A-5
Apply button 3-4
ARP caching 5-21
associations, limiting by MAC address 16-5
attributes, RADIUS
  sent by the access point 12-18
  vendor-proprietary 12-15
  vendor-specific 12-14
authentication
  local mode with AAA 5-16
  NTP associations 5-25
  RADIUS
    key 12-5
    login 5-8, 12-7
  TACACS+
    defined 12-21
    key 12-23
    login 5-13, 12-24
authentication server
  configuring access point as local server 8-2
  EAP 10-4, 12-3
authentication types
  Network-EAP 10-3
  open 10-2
  shared key 10-3
authoritative time source, described 5-23
authorization
  with RADIUS 5-11, 12-11
  with TACACS+ 5-14, 12-21, 12-25
AVVID priority mapping 14-10

B

Back button 3-4
backup authenticator, local 8-1
banners
  configuring
    login 5-42
    message-of-the-day login 5-40
  default configuration 5-40
  when displayed 5-40
basic settings
  checking 22-5
blocking communication between clients 6-15
broadcast key rotation 9-1

C

caching MAC authentications 10-15
Cancel button 3-4
carrier busy test 6-18
CCKM 10-6
CCK modulation 6-7
CDP
  disabling for routing device 17-4

enabling and disabling
on an interface 17-4
monitoring 17-4
Cisco Centralized Key Management
See CCKM
Cisco TAC 22-1
CiscoWorks 2000 18-4
CLI
abbreviating commands 4-3
command modes 4-2
editing features
enabling and disabling 4-6
keystroke editing 4-6
wrapped lines 4-7
error messages 4-4
filtering command output 4-8
getting help 4-3
history
changing the buffer size 4-4
described 4-4
disabling 4-5
recalling commands 4-5
no and default forms of commands 4-3
terminal emulator settings 2-4, 2-6
client ARP caching 5-21
client communication, blocking 6-15
client power level, limiting 6-7
clock
See system clock
command-line interface
See CLI
command modes 4-2
commands
abbreviating 4-3
no and default 4-3
setting privilege levels 5-6
community strings
configuring 18-5
overview 18-3
configuration files
creating using a text editor 20-10
deleting a stored configuration 20-18
downloading
preparing 20-10, 20-13, 20-16
reasons for 20-8
using FTP 20-13
using RCP 20-16
using TFTP 20-11
guidelines for creating and using 20-9
invalid combinations when copying 20-5
system contact and location information 18-9
types and location 20-9
uploading
preparing 20-10, 20-13, 20-16
reasons for 20-8
using FTP 20-14
using RCP 20-17
using TFTP 20-11
connections, secure remote 5-20
crypto software image 5-20
CSID format, selecting 12-13

D

daylight saving time 5-35
default
configuration, resetting 22-5
default commands 4-3
default configuration
banners 5-40
DNS 5-38
NTP 5-25
password and privilege level 5-2
RADIUS 5-8, 12-4
SNMP 18-5
system message logging 21-3
system name and prompt 5-37
TACACS+ 5-13, 12-23

DHCP server
configuring access point as 5-18
receiving IP settings from 2-9
directories
changing 20-4
creating and removing 20-4
displaying the working 20-4
DNS
default configuration 5-38
displaying the configuration 5-40
overview 5-38
setting up 5-39
domain names
DNS 5-38
Domain Name System
See DNS
downloading
configuration files
preparing 20-10, 20-13, 20-16
reasons for 20-8
using FTP 20-13
using RCP 20-16
using TFTP 20-11
image files
deleting old image 20-22
preparing 20-20, 20-23, 20-27
reasons for 20-18
using FTP 20-24
using RCP 20-29
using TFTP 20-21
DTIM 6-16
duplex, Ethernet port 5-15

E

EAP authentication
overview 10-3
EAP-FAST authentication 10-17
EAP-MD5 authentication
setting on client and access point 10-19
EAP-SIM authentication
setting on client and access point 10-20
EAP-TLS authentication
setting on client and access point 10-19
editing features
enabling and disabling 4-6
keystrokes used 4-6
wrapped lines 4-7
EIRP, maximum A-5, A-6, A-7
enable password 5-4
enable secret password 5-4
encrypted software image 5-20
encryption for passwords 5-4
error messages
during command entry 4-4
setting the display destination device 21-5
severity levels 21-7
system message format 21-2
Ethernet indicator 22-3
Ethernet speed and duplex settings 5-15
Ethertype filters 16-11
Express Security page 2-11

F

fallback role 6-3
fast secure roaming 11-1
files
copying 20-5
deleting 20-5
displaying the contents of 20-8
tar
creating 20-6
displaying the contents of 20-6
extracting 20-7
image file format 20-19
file system
displaying available file systems 20-2

displaying file information 20-3
local file system names 20-2
network file system names 20-5
setting the default 20-3
filtering
configuring filters 16-1
Ethertype filters 16-11
IP filters 16-8
MAC address filters 16-3
show and more command output 4-8
Flash device, number of 20-2
fragmentation threshold 6-17
frequencies A-2, A-3, A-4
FTP
accessing MIB files C-2
configuration files
downloading 20-13
overview 20-12
preparing the server 20-13
uploading 20-14
image files
deleting old image 20-26
downloading 20-24
preparing the server 20-23
uploading 20-26

G

get-bulk-request operation 18-3
get-next-request operation 18-3, 18-4
get-request operation 18-3, 18-4
get-response operation 18-3
global configuration mode 4-2
GRE encapsulation 15-6
GRE tunnel 11-14
group key updates 10-14

H

help, for the command line 4-3
history
changing the buffer size 4-4
described 4-4
disabling 4-5
recalling commands 4-5
history table, level and number of syslog messages 21-8
Home button 3-4

I

IGMP snooping helper 14-10
indicators 22-2
inter-client communication, blocking 6-15
interface configuration mode 4-2
IP address, finding and setting 2-20
IP filters 16-8
IPSU 2-19
ISO designators for protocols B-1

K

key features 1-2

L

Layer 3 mobility 11-4, 11-14
LEAP authentication
setting on client and access point 10-17
LED indicators
Ethernet 22-3
radio traffic 22-3
status 22-3
limiting associations by MAC address 16-5
limiting client associations by MAC address 16-5
limiting client power level 6-7

local authenticator, access point as 8-1
login authentication
  with RADIUS 5-8, 12-7
  with TACACS+ 5-13, 12-24
login banners 5-40
log messages
  See system message logging

M

MAC 2-21, 2-22
MAC address ACLs, blocking association with 16-5
MAC address filters 16-3
MAC authentication caching 10-15
management options
  CLI 4-1
Message Integrity Check 9-1
messages
  to users through banners 5-40
MIBs
  accessing files with FTP C-2
  location of files C-2
  overview 18-2
  SNMP interaction with 18-4
MIC 9-1
Microsoft IAS servers 10-2
migration mode, WPA 10-13
mobility, Layer 3 11-14
Mode button 22-8
monitoring
  CDP 17-4

N

Network-EAP 10-3
Network Time Protocol
  See NTP
no commands 4-3
NTP
  associations
    authenticating 5-25
    defined 5-23
    enabling broadcast messages 5-28
    peer 5-27
    server 5-27
  default configuration 5-25
  displaying the configuration 5-32
  overview 5-23
  restricting access
    creating an access group 5-30
    disabling NTP services per interface 5-31
  source IP address, configuring 5-31
  stratum 5-23
  synchronizing devices 5-27
  time
    services 5-23
    synchronizing 5-23

O

OFDM modulation 6-7
OK button 3-4
optional ARP caching 5-22

P

password reset 22-5
passwords
  default configuration 5-2
  encrypting 5-4
  overview 5-2
  setting
    enable 5-3
    enable secret 5-4
    with usernames 5-5
PEAP authentication

setting on client and access point 10-19
ports, protected 6-15
power level
on client devices 6-7
power level, maximum A-5
preferential treatment of traffic
See QoS
pre-shared key 10-14
preventing unauthorized access 5-2
privileged EXEC mode 4-2
privilege levels
exiting 5-7
logging into 5-7
overview 5-2, 5-6
setting a command with 5-6
Public Secure Packet Forwarding 6-15

Q

QoS
configuration guidelines 14-4
overview 14-2
quality of service
See QoS

R

radio
indicator 22-3
radio management 11-1
RADIUS
attributes
CSID format, selecting 12-13
sent by the access point 12-18
vendor-proprietary 12-15
vendor-specific 12-14
WISPr 12-16
configuring
access point as local server 8-2
accounting 12-12
authentication 5-8, 12-7
authorization 5-11, 12-11
communication, global 12-5, 12-13
communication, per-server 12-4, 12-5
multiple UDP ports 12-5
default configuration 5-8, 12-4
defining AAA server groups 5-9, 12-9
displaying the configuration 5-12, 12-17
identifying the server 12-4
limiting the services to the user 5-11, 12-11
method list, defined 12-4
operation of 12-3
overview 12-2
suggested network environments 12-2
tracking services accessed by user 12-12
rate limit, logging 21-9
RCP
configuration files
downloading 20-16
overview 20-15
preparing the server 20-16
uploading 20-17
image files
deleting old image 20-31
downloading 20-29
preparing the server 20-27
uploading 20-31
reauthentication requests 10-2
regulatory
domains A-2, A-3, A-4
reloading access point image 22-8
Remote Authentication Dial-In User Service
See RADIUS
Remote Copy Protocol
See RCP
repeater
as a LEAP client 19-6

as a WPA client 19-7
chain of access points 19-2
restricting access
NTP services 5-29
overview 5-2
passwords and privilege levels 5-2
RADIUS 5-7, 12-1
TACACS+ 5-12
reverse tunnels 15-6
RFC
1157, SNMPv1 18-2
1305, NTP 5-23
1901, SNMPv2C 18-2
1902 to 1907, SNMPv2 18-2
roaming 1-4
fast secure roaming using CCKM 11-1
role in radio network 6-3
rotation, broadcast key 9-1
RTS threshold 6-16

S

scanner mode 1-7
secure remote connections 5-20
Secure Shell
See SSH
security features
synchronizing 10-17
security settings, Express Security page 2-11
self-healing wireless LAN 11-4
sequence numbers in log messages 21-6
service-type attribute 10-2
set-request operation 18-4
severity levels, defining in system messages 21-7
shared key 10-6
show cdp traffic command 17-5
Simple Network Management Protocol
See SNMP
slot time, short 6-18
SNMP
accessing MIB variables with 18-4
agent
described 18-3
disabling 18-5
community strings
configuring 18-5
overview 18-3
configuration examples 18-9
default configuration 18-5
limiting system log messages to NMS 21-8
manager functions 18-3
MIBs
location of C-2
overview 18-2, 18-4
snmp-server view 18-9
status, displaying 18-10
system contact and location 18-9
trap manager, configuring 18-8
traps
described 18-3
enabling 18-7
overview 18-2, 18-4
types of 18-7
versions supported 18-2
snooping helper, IGMP 14-10
software images
location in Flash 20-19
tar file format, described 20-19
spaces in an SSID 7-4
speed, Ethernet port 5-15
SSH 4-9
configuring 5-21
crypto software image 5-20
described 5-20
displaying settings 5-21
SSH Communications Security, Ltd. 4-9
SSID
multiple SSIDs 7-1

troubleshooting 22-5
using spaces in 7-4
static WEP
with open authentication, setting on client and access point 10-17
with shared key authentication, setting on client and access point 10-17
statistics
CDP 17-4
SNMP input and output 18-10
status indicators 22-3
stratum, NTP 5-23
summer time 5-35
switchport protected command 6-16
syslog
See system message logging
system clock
configuring
daylight saving time 5-35
manually 5-33
summer time 5-35
time zones 5-34
displaying the time and date 5-33
overview 5-23
See also NTP
system message logging
default configuration 21-3
defining error message severity levels 21-7
disabling 21-4
displaying the configuration 21-12
enabling 21-4
facility keywords, described 21-11
level keywords, described 21-8
limiting messages 21-8
message format 21-2
overview 21-2
rate limit 21-9
sequence numbers, enabling and disabling 21-6
setting the display destination device 21-5
timestamps, enabling and disabling 21-6
UNIX syslog servers
configuring the daemon 21-10
configuring the logging facility 21-10
facilities supported 21-11
system name
default configuration 5-37
manual configuration 5-37
See also DNS
system prompt
default setting 5-37

T

TAC 22-1
TACACS+
accounting, defined 12-21
authentication, defined 12-21
authorization, defined 12-21
configuring
accounting 12-26
authentication key 12-23
authorization 5-14, 12-25
login authentication 5-13, 12-24
default configuration 5-13, 12-23
displaying the configuration 5-15, 12-27
identifying the server 12-23
limiting the services to the user 5-14, 12-25
operation of 12-22
overview 12-21
tracking services accessed by user 12-26
tar files
creating 20-6
displaying the contents of 20-6
extracting 20-7
image file format 20-19
Telnet 2-23
Temporal Key Integrity Protocol 9-1
Terminal Access Controller Access Control System Plus

See TACACS+
terminal emulator 2-4, 2-6
TFTP
configuration files
downloading 20-11
preparing the server 20-10
uploading 20-11
image files
deleting 20-22
downloading 20-21
preparing the server 20-20
uploading 20-22
TFTP server 22-8
time
See NTP and system clock
timestamps in log messages 21-6
time zones 5-34
TKIP 9-1
traps
configuring managers 18-7
defined 18-3
enabling 18-7
notification types 18-7
overview 18-2, 18-4
troubleshooting 22-1
with CiscoWorks 18-4
with system message logging 21-2

U

UNIX syslog servers
daemon configuration 21-10
facilities supported 21-11
message logging configuration 21-10
upgrading software images
See downloading
uploading
configuration files
preparing 20-10, 20-13, 20-16
reasons for 20-8
using FTP 20-14
using RCP 20-17
using TFTP 20-11
image files
preparing 20-20, 20-23, 20-27
reasons for 20-18
using FTP 20-26
using RCP 20-31
using TFTP 20-22
user EXEC mode 4-2
username-based authentication 5-5

W

WDS 11-1, 11-8
Web-based interface
common buttons 3-4
compatible browsers 3-1
web site
Cisco Software Center 2-20, 22-12
WEP
key example 9-5
with EAP 10-3
WEP key 22-5
Wi-Fi Protected Access
See WPA
Wireless LAN Services Module 11-2
WISPr RADIUS attributes 12-16
world-mode 6-10
802.11d standard 6-10
Cisco legacy 6-10
WPA 10-7
WPA migration mode 10-13